24-3161

United States Court of Appeals for the District of Columbia

THE UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

ROMAN STERLINGOV,

Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA
Hon. Randolph D. Moss
United States District Court Case 1-21-cr-00399-RDM-1

BRIEF FOR DEFENDANT-APPELLANT

TOR EKELAND, ESQ.
TOR EKELAND LAW PLLC
Attorneys for Defendant-Appellant
30 Wall Street, 8th Floor
New York, New York 10005
(718) 737-7264
tor@torekeland.com

MARC FERNICH, ESQ.
LAW OFFICE OF MARC FERNICH
Attorneys for Defendant-Appellant
800 Third Avenue, 20th Floor
New York, New York 10022
(212) 446-2346
maf@fernichlaw.com

MAKSIM NEMTSEV, ESQ.
MAKSIM NEMTSEV PC
Attorneys for Defendant-Appellant
20 Park Plaza, Suite 1000
Boston, Massachusetts 02116
(617) 227-3700
max@mnpc.law

AARON DANIEL, ESQ.
ASYMMETRIC LEGAL
Attorneys for Defendant-Appellant
11900 Biscayne Blvd, Suite 400
Miami, Florida 33181
(305) 979-9296
aaron@asymmetric.legal

(See Inside Cover for Additional Counsel)

3914

ELECTRONIC PARALEGAL

AMY C. COLLINS, ESQ.
THE LAW OFFICE OF
AMY C. COLLINS
Attorneys for Defendant-Appellant
888 17th Street, NW, Suite 1200
Washington DC 20006
(228) 424-0609
amy@amyccollinslaw.com

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rules 28(a)(1) and 32.1, counsel for Plaintiff-Appellant Roman Sterlingov hereby certifies as follows:

I. Parties

The parties appearing before the District Court and all persons who are parties before this Court are as follows:

A. Appellant

Roman Sterlingov

B. Appellee

The United States of America

II. Rulings under Review

This appeal arises from the judgment in a criminal case entered by the U.S. District Court for the District of Columbia on November 13, 2024, in Case No. 1:21-CR-00399.[1] Sterlingov appeals, as argued below, the District Court's:

- denial of his Motion to dismiss filed August 1, 2022 and denied orally from the bench at trial on February 13, 2024, particulary as to venue

[1] A. 091.

and the statute of limitations, as well as the Jury Charge on venue in relation to Count One[2]

- pretrial and trial oral and written admission of Government expert witness testimony under *Daubert*[3]
- denial of Appellant's access to the Chainalysis Reactor closed source code, as well as full access to Reactor's proprietary heuristics
- admission of irrelevant and highly prejudicial evidence of child pornography
- issuance, over objection, of a willful blindness jury instruction
- denial of Appellant's oral motions for a judgment of acquittal at the close of the Government's and Appellant's case in chief[4]
- admission, over objection, of irrelevant, highly prejudicial testimony from cooperating Government criminal witnesses Illya Lichtentstein and Larry Harmon[5]

[2] A. 6567; A. 2626-45.

[3] *See, e.g.,* A. 6951; A. 6400-539.

[4] A. 5386; A. 6140.

[5] A. 4362; A. 4920.

- provisional admission of co-conspirator hearsay statements without foundation and without any fact finding when it permanently admitted the statements into evidence.[6]
- Miscalculation of the "Value of the Laundered Funds" Under U.S.S.G. § 2S1.1(a)(2)[7]

III. Related Cases

The case under review was not previously before this Court or any other court, other than the District Court from which it is appealed and the District Court in the Central District of California where Defendant was originally detained and arraigned.

[6] *See, e.g.,* A. 5227 *et seq.*.

[7] A. 7129-30.

September 15, 2025
Brooklyn, NY

Respectfully submitted:

/s/ Tor Ekeland
Tor Ekeland Law, PLLC
30 Wall Street
8th Floor
New York, NY 10005
Tel: (718) 737-7264
tor@torekeland.com

Attorneys for Appellant-Defendant Roman Sterlingov

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases:

Rules, Laws & Statutes:

Other Authorities:

GLOSSARY

Akemashite Omedetou: "Happy New Year" in Japanese. The pseudonymous moniker for the Bitcoin Talk account the Government argued Sterlingov ran that promoted and discussed Bitcoin Fog. Indirectly attributed to Sterlingov by an "IP Overlap Analysis" by Government expert Mazars.

Apollon Marketplace: A darknet market operating on the Tor network.

Bitcoin: A decentralized digital currency created in 2009 by the pseudonymous Satoshi Nakamoto that allows for transactions without the need for a central administrator, using blockchain technology to record and verify transfers.

Bitcoin Address: A string of letters and numbers used to receive Bitcoin on the Bitcoin blockchain. It is a unique identifier derived from a user's public key. To access Bitcoin sent to that address, the user must possess the corresponding private key, which proves ownership and authorizes transactions. Without the private key, the Bitcoin at that address cannot be spent. Each address is derived from a public key and can be used multiple times.

Bitcoin Core Developer: A Bitcoin Core Developer is a programmer who contributes to the development and maintenance of Bitcoin Core, the reference implementation of the Bitcoin protocol. They are responsible for writing, testing, and improving the software that supports the Bitcoin blockchain and its network, ensuring its functionality, security, and scalability.

Bitcoin Fog: The custodial Bitcoin mixer the Government argues Sterlingov operated.

Bitcoin Mixer: A service that privatizes the transaction history of cryptocurrency by pooling and redistributing Bitcoin among multiple users, making them harder to trace, and adding security for the Bitcoin holder by helping to prevent wrench attacks. Custodial mixers take temporary control of users' coins and redistribute them, while non-custodial mixers use smart contracts or decentralized protocols to mix funds without taking custody.

Bitcoin Talk: An online discussion forum created in 2009 by Bitcoin's pseudonymous founder, Satoshi Nakamoto, and one of the oldest and largest forums dedicated to Bitcoin. It serves as a platform for users to discuss technical developments, trading, security, and broader issues related to Bitcoin and other digital assets. Over time, it has also become a place for announcing new projects, sharing research, and debating policy and regulatory questions. The forum's historical archives are a key source for early documentation of Bitcoin's development and community debates.

Bitfinex: Bitfinex is a major cryptocurrency exchange platform based in Hong Kong that allows users to trade digital assets like Bitcoin. In 2016, the platform was hacked by Government criminal co-operating witness Ilya Lichtenstein, who admitted to laundering approximately 120,000 stolen Bitcoin from the breach using various methods, including Bitcoin mixers.

Blanche Memo:[8] An April 2025 memorandum from DOJ's Deputy Attorney General Todd Blanche, entitled, *Ending Regulation by Prosecution*. It announces a significant shift in DOJ policy regarding digital assets, ending the prior administration’s practice of pursuing regulatory violations through criminal prosecution. Under the memo, federal prosecutors are directed to focus only on cases involving investor harm or the use of digital assets in serious criminal activity, such as terrorism, trafficking, and organized crime. It also disbands the National Cryptocurrency Enforcement Team, instructs prosecutors not to hold mixers responsible for the crimes of their end-users and not to charge digital asset regulatory violations, such as unlicensed money transmission, unless done willfully.

Blockchain: A decentralized, public ledger that permanently records all cryptocurrency transactions in chronological order. The Bitcoin blockchain displays sender and receiver addresses, amounts, and timestamps, but not real-world identities nor geographic locations. While transparent, blockchain data is pseudonymous, and tracing activity on it and making attributions, such as through

[8] A. 7217.

Chainalysis Reactor, largely relies on inferences, assumptions, and information external to the blockchain.

Chainalysis Government Solutions: A for profit, government-facing division of Chainalysis Inc. that provides blockchain tracing software, investigative support, and expert testimony to law enforcement agencies. It uses proprietary tools like Chainalysis Reactor, whose internal methods, data sources, and error rates are not publicly available or independently verified.

Chainalysis Reactor: A closed-source, proprietary blockchain analytics software developed by the private for-profit company Chainalysis Inc., used to trace cryptocurrency transactions and make attributions. Reactor employs a combination of heuristics, including co-spend analysis, behavioral pattern recognition, and off-chain data drawn from undisclosed sources, to probabilistically cluster cryptocurrency addresses and associate them with specific entities or services. The software's internal algorithms and data sources are proprietary and have not been subject to independent testing or peer review. Reactor cannot determine any geographic locations of any transaction or user. In this case, the Government's expert witnesses relied heavily on Reactor to support their conclusions, despite the software's lack of scientific transparency, known accuracy metrics, or general acceptance in the relevant scientific community.

Change Address: A change address in Bitcoin is a new address generated by a wallet to receive leftover funds from a transaction, similar to getting coins back after paying with a large bill. Change addresses are necessary because Bitcoin transactions don't allow users to send an exact amount from a portion of their balance, entire inputs must be spent, and the difference is returned to the sender as change at a new address. This process is automatic and common, but it complicates blockchain analysis because it creates additional addresses that may or may not be clearly linked to the original sender. Chainalysis Reactor assumes that the address receiving this change output is controlled by the same entity as the sending address, and uses this assumption to cluster addresses.

Cluster: A group of cryptocurrency addresses attributed to a single entity by blockchain tracing software like Chainalysis Reactor. Cluster attributions are assumed using heuristics based on transaction patterns and proprietary data.

Closed Source: Closed source software is software whose source code is not shared with the public and is typically restricted by licensing agreements. Users can run the software, but they cannot inspect, modify, or distribute its underlying code.

Coinapult: Coinapult was a web-based Bitcoin wallet and payment service that allowed users to store, send, and receive Bitcoin online. It also offered a feature called "Locks," enabling users to peg their Bitcoin value to fiat currencies or commodities to avoid price volatility. Coinapult ceased operations in early 2021.

The company shut down its services and began liquidating user accounts after years of declining activity and increasing regulatory pressures. The Government used Coinapult in their 2016 mix of Government Bitcoin through Bitcoin Fog.

CoinJoin: A Bitcoin privacy technique that combines multiple users' transactions into a single transaction with multiple inputs and outputs, making it harder to determine which input corresponds to which output. CoinJoins are designed to break the link between sender and receiver, undermining clustering assumptions like the "co-spend" heuristic.

Consolidation Address: A consolidation address is a cryptocurrency address used to collect and pool funds from multiple incoming transactions into a single location.

Co-Spend Heuristic: A blockchain analysis method that observes when multiple cryptocurrency addresses are used together as inputs in a single transaction and reaches conclusions based on this. Chainalysis Reactor assumes that the co-spent addresses are controlled by the same entity and uses this assumption as the foundation of its primary clustering technique.

Custodial Mixer: A custodial mixer is a service that temporarily holds users' cryptocurrency and redistributes it to designated addresses in a way that obscures the link between sender and recipient. By breaking the direct chain of transactions, custodial mixers help protect personal financial privacy on the otherwise publicly visible blockchain.

Darknet: The darknet is the portion of the internet that is not indexed by traditional search engines like Google or Bing and requires particular publicly available software, such as the Tor browser or I2P, to access. It is often used to host websites and services that prioritize anonymity and privacy. While it has been associated with illicit activity, it also provides a platform for legitimate uses such as secure communications, political activism, and privacy protection.

Darknet Market: A darknet market is an online marketplace hosted on encrypted networks like Tor, where users often, but not exclusively, trade illicit goods or services, including drugs, weapons, or stolen data, as well as legitimate goods and services. These markets operate anonymously, using cryptocurrencies like Bitcoin for transactions.

Decentralized Ledger: A decentralized ledger is a digital record-keeping system distributed across multiple nodes or computers, with no central authority controlling the data. Each participant in the network maintains a synchronized copy of the ledger, ensuring transparency, security, and resistance to tampering.

DNS Registration: DNS registration is the process of associating a domain name with a specific IP address by recording it in the Domain Name System (DNS), allowing users to access websites using human-readable names like *example.com*.

This registration includes details such as the registrant's contact information, registration date, and the domain's linked name servers.

Domain Name: A domain name is a human-readable address used to identify a website on the internet, such as *example.com*. It serves as a shortcut to an IP address, making it easier for users to access online resources without remembering numeric codes.

Error rate: Error rate refers to the frequency at which a system or method produces incorrect results, typically expressed as a percentage of total operations. In forensic or analytical tools, a high error rate undermines reliability and accuracy.

False Negatives: In forensic investigations, a false negative occurs when a test or analysis fails to detect evidence that is actually present. This can lead to incorrect conclusions, such as mistakenly excluding a suspect or overlooking relevant data.

False positive rate: False positive rate is the proportion of instances where a system incorrectly identifies something as true or present when it is not. In the context of blockchain analysis, it reflects how often addresses or transactions are wrongly attributed.

Fiat Currency: Government-issued money that is not backed by a physical commodity such as gold or silver. Its value is established by government regulation and public confidence rather than intrinsic value. The U.S. Dollar is fiat currency.

Helix Mixer: Helix was a Bitcoin mixer designed to anonymize cryptocurrency transactions by obscuring the origin and destination of funds. Its operator, testifying and Government criminal co-operating witness Larry Harmon, was arrested in 2020 for laundering over $300 million worth of Bitcoin through Helix, including funds tied to darknet markets.

Heuristics: Rule-of-thumb methods or shortcuts that rely on assumptions to identify patterns or make decisions when exact data is unavailable. In blockchain analysis, heuristics are used to infer relationships between addresses and make attributions, but these inferences rest on assumptions that can be error-prone and are often not transparent.

Hops: In Bitcoin, "hops" refer to the number of transactions or intermediary Bitcoin addresses that occur between a source address and a destination address during the movement of Bitcoin. Each hop represents a step in the transaction chain, and the more hops there are, the harder it becomes to reliably trace or attribute the flow of Bitcoin to a specific individual.

Input: In Bitcoin blockchain tracing, an input refers to the source of Bitcoin used in a transaction, specifically, the previously received Bitcoin being spent. Each input points to an earlier transaction's output, and tracing inputs allows analysts to follow the flow of funds backward through the blockchain.

IP Address: Short for internet protocol address, it is a numerical identifier assigned to a device connected to the internet or a local network, used to facilitate data transmission between devices. Although sometimes used in forensic analysis to infer a user's location or identity, an IP address does not uniquely identify a specific individual, device, or geographic location and is easily spoofed. Multiple users can share a single IP address (e.g., via public Wi-Fi), and anonymization technologies like VPNs and the Tor network can obscure or mask true IP address origins. In this case, the Government relied on a novel, ad-hoc and untested "IP address overlap" analysis to make implicit attributions or internet accounts to Sterlingov, despite the inherent limitations and unreliability of such inferences without corroborating evidence.

IP Overlap Analysis: A novel, one-off methodology developed by FBI Computer Scientist Mazars specifically for this case, which attempted to link Sterlingov to Bitcoin Fog by identifying shared IP addresses used by both his known accounts and pseudonymous accounts associated with the service. The analysis involved comparing login data across multiple platforms to find temporal overlaps in IP usage. Mazars admitted it was the first time she had ever done it, that she made it up for this case, that it had no scientific basis, that it was not a scientific method, that it had never been peer-reviewed or validated, and that it did not establish direct attribution or control, and that it rested entirely on speculative correlations.

Kraken: Kraken is a U.S.-based cryptocurrency exchange that allows users to buy, sell, and trade a wide range of digital assets, including Bitcoin and Ethereum. It also offers services such as margin trading, staking, and fiat currency deposits and withdrawals.

LocalBitcoins.com: LocalBitcoins.com was a peer-to-peer cryptocurrency exchange platform that allowed users to buy and sell Bitcoin directly with one another, often using cash or other payment methods. The platform acted as an escrow service to hold funds during transactions but did not take custody of user wallets. It ceased operations in 2023.

Logs: Logs are records automatically generated by computer systems or software that document events, user activity, or system operations over time. They are often used for monitoring, troubleshooting, and forensic analysis.

Output: In Bitcoin blockchain tracing, an output is the destination of Bitcoin in a transaction, specifying the amount of Bitcoin sent and the recipient's address. Outputs can either be spent in future transactions (becoming inputs) or remain unspent, forming what is known as an unspent transaction output (UTXO).

PayJoin: A PayJoin (also known as Pay-to-EndPoint or P2EP) is a type of collaborative Bitcoin transaction where both the sender and receiver contribute inputs, breaking common heuristics used to track ownership and improve privacy.

Unlike standard transactions, PayJoins obscure the origin of funds, making blockchain analysis significantly more difficult.

Peer-to-Peer: A network model in which participants interact directly with each other rather than through a central authority or intermediary. In the context of digital currencies, peer-to-peer systems allow users to send and receive payments directly over the network without relying on banks or payment processors.

Private Key: In Bitcoin, private keys are secret cryptographic codes that allow a user to authorize and control transfers from a specific Bitcoin address. Possession of the private key is required to initiate a valid transaction on the blockchain. Private keys are not stored on the blockchain and are kept by the user. Chainalysis Reactor assumes that if multiple Bitcoin addresses are used together in a transaction (a "co-spend"), the same user must control all corresponding private keys, an unverified assumption central to Chainalysis Reactor's clustering method. Possession of a private key establishes possession and control of the related Bitcoin.

Proxy server: An intermediary computer system that routes requests between a user and the internet, masking the user's IP address. It can provide privacy, security, or access control, but also may be used to conceal identity or location.

Post-mix: Post-mix transactions refer to the movement of cryptocurrency after it has passed through a mixing service, at which point it is disbursed to addresses controlled by the user. These transactions occur outside the mixer and are entirely determined by the user, not the mixing service.

Public Key: A public key in Bitcoin is a cryptographic code generated from a private key that allows others to send Bitcoin to a user's address. A public key is stored on the blockchain. It serves as the basis for creating a Bitcoin address but cannot be used to access or spend funds on its own for which a private key is required.

Servers: Powerful computers or systems that provide data, services, or resources to other computers, known as clients, over a network. In the context of websites or online services, servers host content, run applications, and handle user requests.

Server logs: Server logs are specific types of logs maintained by a server, recording details such as user access, IP addresses, time stamps, and actions taken on the hosted service. These logs can be crucial in tracing activity and understanding how a service was used. The Government produced no original server logs in this case, and Mazar testified that she had no access to original logs when she wrote her IP Overlap Analysis.

shormint.com@hotmail.com: An email address the Government argued Sterlingov controlled on the basis of Mazars' IP Overlap Analysis.

Tor Browser: A web browser designed to access the Tor network, routing internet traffic through multiple encrypted relays to anonymize users' identities and locations. Originally developed by the U.S. Naval Research Laboratory, it is now maintained by The Tor Project, a nonprofit organization dedicated to online privacy and freedom. The Tor Browser is commonly used to access both the open web and hidden services on the darknet. It is commonly used by governments, political dissidents, journalists, and democracy advocates around the world.

Tor Network: A privacy-focused internet network that routes traffic through multiple encrypted layers to obscure users' identities and locations. Originally developed by the U.S. Naval Research Laboratory to protect government communications, Tor is now publicly accessible and widely used for anonymous browsing.

Unspent Transaction Output (UTXO): A chunk of Bitcoin that has been received in a transaction but not yet spent. It represents the amount of digital currency available to a user and is used as the input in a future transaction.

VPN: Short for virtual private network, it is a service that creates a secure, encrypted connection between a user's device and the internet, masking the user's IP address and location. VPNs are commonly used by businesses adn the public to protect privacy, bypass geographic restrictions, and secure data on public networks.

Wallet: A Bitcoin wallet is a software application or hardware device that stores a user's private keys and allows them to send, receive, and manage their Bitcoin. It does not hold the coins themselves, but rather the private keys needed to access and authorize transactions on the blockchain.

Welcome to Video: A South-Korean darknet website that facilitated the distribution of CSAM and accepted Bitcoin as payment. It was dismantled in 2018 as part of a coordinated international law enforcement effort.

Wrench Attack: A wrench attack refers to a physical threat, such as violence or coercion, used to force someone to give up access to their cryptocurrency, typically by revealing their private keys. They are a reason people use mixers to mask the amount of Bitcoin they hold.

JURISDICTIONAL STATEMENT

This appeal arises from the Judgment in a Criminal Case entered by the U.S. District Court for the District of Columbia on November 13, 2024, in *U.S. v. Roman Sterlingov*, Case No.1:21-cr-00399.[9] The District Court had jurisdiction under 18 U.S.C. § 3231. This Court has jurisdiction under 28 U.S.C. § 1291. Sterlingov was sentenced to 150 months.[10] On November 20, 2024, Sterlingov filed a timely Notice of Appeal.[11]

[9] A. 091.

[10] A. 093.

[11] A. 7214.

PERTINENT STATUTES AND REGULATIONS

18 U.S.C. § 1956(h) – Money Laundering Conspiracy (Count 1)

18 U.S.C. § 1956(a)(3)(A), (B) – Money Laundering (Count 2)

18 U.S.C. §§ 1960(a) & (2) – Operating an Unlicensed Money Transmission Business & Aiding and Abetting (Count 3)

D.C. Municipal Code § 26-1023(c) – Money Transmission Without a License Within the District of Columbia (Count 4)

18 U.S.C. § 982(a)(1) – Forfeiture

21 U.S.C. § 853(p) – Substitute Forfeiture

STATEMENT OF ISSUES

1. **Whether venue was unconstitutional in the District of Columbia?**

2. **Whether the District Court erred under *Daubert* in admitting expert testimony and evidence related to blockchain tracing?**

3. **Whether the District Court erred under *Daubert* in admitting expert testimony and evidence related to the novel IP Overlap Analysis?**

4. **Whether the denial of access to the Chainalysis Reactor Source Code and complete set of heuristics violated Appellant's Sixth Amendment Confrontation Clause rights, and Fifth Amendment due process right to put on a complete defense?**

5. **Whether the District Court abused its discretion by admitting irrelevant and prejudicial evidence concerning child pornography?**

6. **Whether the Government constructively amended the Indictment with its child pornography evidence?**

7. **Whether the District Court erred in giving a willful blindness jury instruction?**

8. **Whether the evidence was insufficient to support the verdict?**

9. **Whether the District Court erred in admitting the testimony of Government cooperating witnesses Lichtentstein and Harmon?**

10. **Whether the District Court erred in provisionally, then finally, admitting alleged co-conspirator statements?**

11. **Whether the District Court miscalculated the value of the laundered funds Under U.S.S.G. § 2S1.1(a)(2)?**

12. **Whether the charged crimes occurred outside the statute of limitations?**

STATEMENT OF THE CASE

On April 27, 2021, Appellant Roman Sterlingov, a dual Swedish-Russian national, was arrested at Los Angeles International Airport and charged with a series of offenses related to the operation of the Bitcoin Fog mixer Bitcoin Fog. Bitcoin mixers are legal.[12] A Bitcoin mixer provides a user with financial privacy on an otherwise public blockchain ledger, preventing bad actors from learning the amount of Bitcoin a person may have by tracing their transaction history.[13] Over the years Bitcoin owners have been subject to what are known as wrench attacks, where they are physically targeted by assailants seeking their private digital keys to obtain control of their Bitcoin addresses, and hence their wealth.[14]

Sterlingov lived in Sweden since the age of 14.[15] Before his arrest, he resided in Gothenburg, a university town in Sweden. He developed an interest in computers

[12] *See, e.g.,* A. 6224; A. 6240; A. 6705; Hrg. Tr. at 45:3 (Oct. 25, 2021) ("There's nothing per se illegal about mixing Bitcoins" AUSA C. Brown); A. 3718 (District Court saying mixing isn't illegal per se).

[13] *See, e.g., What Is a Bitcoin Mixer?* COINBASE LEARN YOUR CRYPTO, https://www.coinbase.com/learn/your-crypto/what-is-a-bitcoin-mixer (last visited Sept. 9, 2025).

[14]*See, e.g,.* Paul Vigna, *Severed Fingers and 'Wrench Attacks' Rattle the Crypto Elite*, WALL ST. J. (July 20, 2025), https://www.wsj.com/finance/currencies/crypto-industry-robberies-attacks-32c2867a (last visited Sept. 9, 2025).

[15] A. 198.

at a young age and became involved with Bitcoin in 2010.[16] Before his arrest, he had never set foot in Washington, D.C., nor had any contacts with the District.

Sterlingov was convicted in an unconstitutional venue, entirely on post-hoc, circumstantial forensic evidence and speculation, unreliable under *Daubert*, for the alleged money laundering crimes of Bitcoin Fog's end-users. There is no evidence of any of those end-users being in D.C. except for Government investigators mixing licit Government Bitcoin through Bitcoin Fog, without any evidence that Sterlingov was aware of the mixes, or of any representation by the Government that the Bitcoin was illicit. DOJ has since disavowed prosecutions of mixer operators for the crimes of their end-users.[17] The District Court compounded the errors in this case by, among other things: admitting irrelevant and inflamatory evidence of child pornography unrelated to Sterlingov; improperly giving a willful blindness instruction to the jury; allowing irrelevant and prejudicial witness testimony; and improperly calculating the value of funds allegedly laundered. On whole, the evidence is insufficient to sustain the verdict. Finally, there is a question whether any of the charged crimes occurred within the statute of limitations.

[16] A. 201.

[17] A. 7217.

BACKGROUND

On April 27, 2021, the Government arrested Sterlingov at Los Angeles International Airport.[18] On July 18, 2022, Sterlingov was charged in a Superseding Indictment in this District with four counts: (1) conspiracy to commit money laundering, (2) money laundering, (3) operating an unlicensed money transmitting business, and (4) conducting money transmission without a license in violation of a D.C. municipal statute.[19] At all relevant times Sterlingov was outside this District, either in Sweden or travelling outside the U.S., with the exception of a trip to Miami in 2017 when the Government placed him under surveillance but neither arrested him nor introduced any evidence from this surveillance at trial.[20]

The Government's theory was that Sterlingov operated the Bitcoin Fog mixer with co-conspirators, thereby facilitating the laundering of illicit proceeds and running an unlicensed money transmission business in D.C. At trial there was no direct evidence linking Sterlingov to the operation of Bitcoin Fog, or any co-conspirators, beyond speculative attributions based on untested, unscientific, novel, forensics. No eyewitnesses testified to Sterlingov operating Bitcoin Fog, and no

[18] A. 6542; A. 6556.

[19] A. 6561.

[20] A. 3031-32.

victims testified. All the Government witnesses consisted of forensic experts, investigators, irrelevant cooperating witnesses, and translators, all coming in years after the fact. The Government did not introduce the Bitcoin Fog servers into evidence, nor its server logs, ledger, any private keys related to its operation, or communications between Sterlingov and any co-conspirators. This is despite seizing numerous electronic devices and property from Sterlingov upon his arrest - including a spreadsheet of his internet passwords.[21]

Although the Government cooperated with Swedish law enforcement, including getting Swedish law enforcement to surveill Sterlingov, it never seized his computers from his apartment in Sweden after his arrest, nor introduced any evidence from Swedish law enforcement's surveillance.[22] Additionally, the Government had Romanian law enforcement surveill the signal traffic to and from a server Sterlingov had in Romania for a VPN business he ran, that the Government mistakenly believed to be the Bitcoin Fog servers, but likewise introduced no evidence from this surveillance at trial.[23]

[21] *See, e.g.,* A. 6529; A. 6531; A. 4864.

[22] A. 3031-42; A. 3046.

[23] A. 3042.

The sole basis for venue in this District as alleged in Count Two of the Indictment comes from November 2019, when IRS CI Price sent a message from this District to the Bitcoin Fog help desk saying he wanted to launder drug money.[24] There is no evidence that the message was received or read by anyone, or even that the help desk was operational at this time.[25] Price then mixed roughly $86 of Bitcoin from a Government Apollon marketplace account through Bitcoin Fog without any indication that the Bitcoin was related to the message. There is no evidence that Bitcoin involved in any of the Government's Bitcoin Fog mixes were illicit. Price had mixed Government Bitcoin one other time prior without sending a message or any evidence that the funds were illicit.[26] Government witness AUSA Comolli (an FBI agent at the time she testified about) also testified she mixed Government Bitcoin once through Bitcoin Fog, without sending a message, or any evidence that the Bitcoin used was illicit.[27] This is the only evidence of anything happening in D.C. over the Government's investigation spanning a decade.

[24] A. 2833 *et seq.*

[25] A. 3038.

[26] A. 3037-38.

[27] A. 5216.

On August 1, 2022, Sterlingov moved to dismiss on venue and statute of limitations grounds, among other things.[28] The District Court never issued a written ruling and orally denied the motion from the bench during trial on February 13, 2024, more than a year after its filing.[29]

Due to the novel, unregulated, and unscientific nature of the Government's blockchain forensics, mainly consisting of outputs from proprietary blockchain surveillance software Chainalysis Reactor, and a novel, unscientific "IP Overlap Analysis," the Defense requested and was granted pretrial *Daubert* hearings.[30]

During the *Daubert* proceedings, the District Court displayed a lack of understanding of the fundamental aspects of Bitcoin's blockchain technology. The court asked whether the blockchain has an administrator. [31] It is a basic fact that the Bitcoin blockchain has no administrator as it is a decentralized ledger.

The District Court did not issue a written *Daubert* ruling until the day before the Government's Chainalysis tracing expert, Elizabeth Bisbee, testified at trial.[32]

[28] A. 6567.

[29] A. 2626-45.

[30] *See, e.g.,* A 503-656; A. 1356-1409.

[31] A. 552.

[32] A. 6951.

The order was limited to the admissibility of Bisbee's testimony and that of the primary blockchain forensic software used by the Government in this case, Chainalysis Reactor. Based largely on law enforcement anecdotes, as there was no scientific evidence for Reactor's reliability, the District Court admitted Bisbee's and Reactor's testimony.

Chainalysis Reactor, a closed-source blockchain tracing tool that relies on proprietary heuristics, lies at the core of the Government's case.[33] It was used for tracing and attributing darknet cash flows to and from - but not through - Bitcoin Fog. Bisbee testified that neither she nor Chainalysis Reactor made any attribution that Sterlingov was the operator of Bitcoin Fog.[34] She also admitted during both her *Daubert* hearing and trial that the Reactor had not undergone peer review or internal error analysis, and that its error rates and accuracy regarding false positives or negatives was unknown.[35] She further conceded that Reactor cannot distinguish transactions by geography or legal jurisdiction, and that its proprietary code is closed off from outside scrutiny, preventing independent verification of its accuracy.[36]

[33] *See, e.g.,* A 6400; A 6465; A 6493; A 6522.

[34] A. 608.

[35] *See, e.g.,* A 619; A. 639-40; *see also* A 622-23; A 627-28.

[36] A. 5164; *see also* A. 4143.

The Defense was denied meaningful access to Reactor's proprietary heuristics and closed source code due to, among other things, an overly restrictive and punitive non-competition clause in a proposed protective order that the Defense and Defense experts refused to sign.[37] The clause barred signors from working for any Chainalysis competitor during the litigation and for five years afterward, effectively deterring qualified experts with the threat of litigation from the multi-billion dollar Chainalysis, Inc.[38] This left the Defense unable to fully challenge the Government's forensic evidence.[39] Fear of litigation by Chainalysis appears also to have been behind the Defense's blockchain tracing expert Jonelle Still's last-minute refusal to testify.[40]

The primary circumstantial evidence tying Sterlingov to Bitcoin Fog came from FBI computer scientist Mazars' novel IP Overlap Analysis that she used to imply a connection between Sterlingov and a pseudonymous email - shormint@hotmail.com - linked to Bitcoin Fog.[41] Under cross-examination, she

[37] *See, e.g.,* A 6884; *below* Part II.

[38] *See, e.g.,* A. 6864.

[39] *See, e.g.,* A. 2331; A 6843.

[40] A 6884.

[41] *See, e.g.,* A. 1356; A 4840; *below*, Part II.

conceded that her method was a novel, one-off technique she created solely for this case.[42] She admitted it was not a scientific methodology and that she did not know its error rates.[43] She admitted at her Daubert hearing and trial that she did not attribute the shormint@hotmail.com email address to Sterlingov.[44]

Mazars gave false testimony at trial that the Government had to retract. She testified that Sterlingov had discussed money laundering in a chat message that the Government subsequently introduced into evidence as Government Exhibit 721.[45] However, on cross-examination, she was testified that the alleged message was actually copied, and cropped in a way to make it look like a real chat, from a dating advice e-book and was not an authentic chat log at all. [46] A fact she failed to verify before trial. She also erroneously testified that she was unable to review a 6 Terabyte encrypted hard drive listed on her device review summary, allegedly seized from Sterlingov at the airport, but then admitted on the stand that it was not Sterlingov's hard drive at all but rather a Government one.[47] Additionally, Mazars confirmed that

[42] *See, e.g.,* A. 4853-57.

[43] *See id.*

[44] A. 1397; A 4855.

[45] A. 4798-4805; A. 7414.

[46] *See* A. 5905-5915; *see also,* A. 6144-47; A 7253; A. 7414.

[47] A. 4862-64.

the Government did not have the Bitcoin Fog's server, source code, logs, ledger nor any communications linked to Bitcoin Fog.[48]

Aside from Mazars and Bisbee, the Goverment's primary expert was Luke Scholl of the FBI, who testified over objection as an expert on blockchain tracing.[49] He primarily used Chainalysis Reactor to trace Bitcoin linked to darknet marketplaces and Bitcoin Fog, and wrote a report admitted into evidence.[50] He testified that no reference to Bitcoin Fog was discovered in any of Sterlingov's devices.[51] He acknowledged that tracing relies on external corroboration, such as undercover purchases and seized records, because blockchain data alone is insufficient to identify specific users or operators.[52] Scholl testified that tracing is speculative, that Chainalysis clustering could miss relevant addresses, and that his analysis did not directly connect Sterlingov to the operation of Bitcoin Fog.[53] His

[48] A. 4860.

[49] *See, e.g.,* A. 541; A 6400.

[50] A. 6400.

[51] A. 4172.

[52] *See, e.g.,* A. 4206; A 4146-48.

[53] A. 4146-48.

conclusions were based on general transaction patterns, rather than any specific evidence tying Sterlingov to the site.

Scholl also testified that the Government did not have Bitcoin Fog's server, source code, or ledgers.[54] Scholl testified as to 10 darknet markets, almost all shut down before the relevant statute of limitations. Scholl confirmed that blockchain clustering relies on assumptions, such as grouping all addresses in a cluster under one user, that may not always hold true.[55]

During cross-examination, Scholl testified that the "hops" in his blockchain tracing referred to intermediary steps between Bitcoin Fog addresses and those linked to Sterlingov.[56] He acknowledged that these hops did not reflect a direct link between Bitcoin Fog and Sterlingov and were based on his interpretation of Reactor's output.[57] He testified that these hops consisted of multiple intermediary

[54] A. 4200.

[55] A. 4146-48.

[56] *Id.*

[57] *Id.*

addresses for which the Government did not have the private keys.[58] Scholl said that misidentifying a change address could alter the results of the tracing.[59]

Scholl testified that possessing a private key is the most concrete way to establish control of a Bitcoin address, but that blockchain forensics rely on circumstantial off-chain evidence to make attributions.[60] He corroborated Price's and Mazars's testimony that the Government did not find private keys to any Bitcoin Fog addresses on Sterlingov's devices, and that absent such evidence, attribution is speculative.[61] Scholl further conceded that the transfer of private keys between individuals is not recorded on the blockchain, making it impossible to detect such activity from blockchain analysis alone.[62]

Agent Leo Rovensky testified as a summary witness regarding blockchain tracing and financial records but he repeatedly crossed into speculative territory, drawing repeated objections from the Defense finally leading the court to strike part of Rovensky's testimony and give a curative instruction clarifying that Rovensky

[58] *See*, *e.g.*, A 4179-62.

[59] *See, e.g.*, A 4159-62.

[60] *See* A. 4159-62.

[61] *See* A. 4159-62.

[62] *See* A. 4180.

was not an expert.[63] He acknowledged that key records, such as internal server logs, administrator communications, or transaction ledgers, were never recovered, and that none of Sterlingov's electronic devices contained any data tying him to the site.[64]

Rovensky also confirmed that the pseudonymous email accounts central to the Government's theory, including shormint@hotmail.com and others, were never found on Sterlingov's devices or linked to him through subscriber data.[65]

At trial, the Government sought to admit co-conspirator statements under Fed. R. Evid. 801(d)(2)(E) – essentially all the hearsay evidence related to the darknet markets - without first establishing the necessary foundational elements that a conspiracy existed, that Sterlingov knowingly joined it, and that the statements were made in furtherance of that conspiracy. The court provisionally admitted the statements, subject to the Government later laying a foundation.[66]

[63] A. 3295-97; A. 3258-97.

[64] A. 3577-3584.

[65] A. 3581-84.

[66] *See, e.g.,* A. 3927-28; *below* Part VIII.

FBI Agent Steven Santell testified at length, over repeated objection, regarding darknet markets involving narcotics and other illicit goods.[67]

[67] A. 5227 *et seq.*

ARGUMENT

Venue is unconstitutional in D.C. because no crime occurred here, nor any act in furtherance of any crime. The only evidence of anything happening in D.C. consisted in unilateral acts of Government agents mixing Government Bitcoin with Bitcoin Fog three times over three years. There is no evidence the Bitcoin used were illicit, or that Sterlingov, or anyone else, was aware of the Government's mixing.

No eyewitnesses testified, and no evidence came in of Sterlingov operating Bitcoin Fog. The Government's case consisted of forensic speculation years after the fact based on unscientific, unregulated, and novel methodologies.

Additionally, the District Court erred by forbidding the Defense access to the heuristics and source code for the proprietary Chainalysis Reactor blockchain forensic software. This violated Sterlingov's Sixth Amendment Confrontation Clause rights and his Fifth Amendment due process rights to put on a complete defense.

No victims were identified, and none testified. Yet, the District Court admitted prejudicial and irrelevant evidence related to child pornography.

The District Court further erred in instructing the jury on willful blindness, a disfavored doctrine that equates deliberate ignorance with actual knowledge, despite lacking the required factual basis.

The District Court also erred in admitting irrelevant and prejudicial testimony of Government criminal cooperating witnesses who had no connection to Sterlingov and who gave improper expert testimony despite being lay witnesses.

Viewed as a whole, the trial record is insufficient to support the verdict. Post-trial the District Court miscalculated the value of laundered funds. Finally, the record is insufficient to support the proposition that any of the charged crimes occurred in D.C. within the requisite statutes of limitations.

For these reasons, as argued below, this Court should vacate the Judgment and dismiss the Indictment.

I. Venue is Unconstitutional

Venue is unconstitutional in D.C. under any applicable test. No crime occurred in this District, nor anything in the furtherance of the conspiracy. There is no evidence of any conduct by Sterlingov, or any co-conspirator, in, or directed to, this District. The only thing that happened in this District were three Government Bitcoin mixes through Bitcoin Fog that there is no evidence were illicit or that anyone besides the Government knew of.

The Government's three mixes, once in 2016 and twice in 2019, are the only things that happened in D.C.[68] There is no evidence the mixed Bitcoin was illicit.[69] These unilateral Government actions, absent any evidence of Sterlingov's *mens rea*, cannot constitutionally support venue. They do not constitute money laundering, nor its representation, because there is no evidence that anyone ever received or saw the single message sent by the Government to Bitcoin Fog in 2019. Because Bitcoin Fog never directed any activity towards this District, nor was located in it, it can not be said to be have been doing business in this District. The record is insufficient to support venue under any constitutional test because no crimes, nor anything in furtherance of any crime, occurred in this District.[70]

The Constitution's venue provisions, along with Fed. R. Crim. P. 18 exist to prevent prejudicial governmental gaming of venue.[71] The Constitution's two venue

[68] A. 3037-38; A. 5216.

[69] A. 3037-38.

[70] *See, e.g., U.S. v. Auernheimer*, 748 F.3d 525, 532–37 (3d Cir. 2014).

[71] *See, e.g.*, *Smith v. U.S.*, 599 U.S. 236, 248 (2023).

clauses are rooted in the venue abuses of the English Crown that help spark the American Revolution.[72] Venue is no mere technicality.[73]

To uphold venue in this case is to give law enforcement a blank check in internet cases to create venue merely by unilaterally interacting with an internet site without its owner's knowledge, and in essence, creating a strict liability crime.

A. Standard of Review

Where a jury instruction on venue has been properly given, this Circuit reviews whether any rational trier of fact could have found venue proper by a preponderance of the evidence, viewing the record in the light most favorable to the Government.[74] Where Congress does not provide a statutory venue provision, courts use the *locus delicti* test: examining the nature of the alleged crime and the location or locations of the acts constituting it.[75]

[72] U.S. Const. art. III, § 2, cl. 3; U.S. Const. amend. VI; Fed. R. Crim. P. 18; *see, U.S. v. Cabrales*, 524 U.S. 1, 6 (1998); *Auernheimer*, 748 F.3d at 532; The Declaration of Independence para. 21 (U.S. 1776).

[73] *See Auernheimer*, 748 F.3d at 532.

[74] *See U.S. v. Morgan,* 393 F.3d 192, 195 (D.C. Cir. 2004); *U.S. v. Lam Kwong-Wah*, 924 F.2d 298, 301–02 (D.C. Cir. 1991).

[75] *See U.S. v. Rodriguez-Moreno*, 526 U.S. 275, 279 (1999); *U.S. v. Cabrales*, 524 U.S. 1, 6–7 (1998); *U.S. v. Anderson*, 328 U.S. 699, 703 (1946); *Morgan*, 393 F.3d at 196.

B. Venue is Strictly and Narrowly Construed

Venue in criminal cases must be strictly and narrowly construed to protect the accused's constitutional right to be tried in the vicinage where the alleged offense occurred.[76] Venue only attaches to essential conduct, not ancillary effects, or unilateral government-investigative activity.[77]

Recently, the S.D.N.Y. in the cryptocurrency case *Eisenberg* vacated the conviction on venue grounds, because none of the essential conduct elements occurred in the district.[78] In the internet case *Auernheimer*, the Third Circuit vacated because venue was improper where no essential conduct or substantial contacts occurred in New Jersey.[79] In *Fortenberry*, the Ninth Circuit reversed, holding that an effects-based theory, premising venue solely on the presence of investigators in

[76] *See Morgan*, 393 F.3d at 195-96; *Smith v. U.S.*, 599 U.S. 236, 248 (2023); *U.S. v. Johnson*, 323 U.S. 273, 276 (1944); *see also, Auernheimer*, 748 F.3d at 532.

[77] *See U.S. v. Swann*, 441 F.2d 1053, 1054–55 (D.C. Cir. 1971); *Lam Kwong Wah*, 924 F.2d at 301–02; *U.S. v. Gamble*, No. 19-cr-348 (CKK), 2020 WL 3605829, at *5 (D.D.C. July 2, 2020); *U.S. v. Fortenberry*, 89 F.4th 702, 709-10 (9th Cir. 2023).

[78] *See U.S. v. Eisenberg***,** No. 23-cr-10 (AS), 2025 WL 1489248 at *21, (S.D.N.Y. May 23, 2025).

[79] *Auernheimer***,** 748 F.3d at 531.

the trial district, rather than any conduct by the defendant, had "no support in the Constitution, in federal statute, or in historical practice."[80]

1. Venue is Unconstitutional for Count One Because There was No Conspiratorial Conduct in D.C.

There is no evidence of any conspiratorial agreement or act in D.C. involving Sterlingov or any co-conspirator.

18 U.S.C. § 1956(h) requires no overt conspiratorial act.[81] 18 U.S.C. § 1956(i) designates venue in any district where an overt act in furtherance of the conspiracy occurred, even though an overt act is not a required element of the conspiracy itself.[82] But there is no evidence of any agreement or conduct occurring in D.C by Sterlingov or any co-conspirator. The only acts in this district were conducted by Government agents without the knowledge of Sterlingov or any co-conspirator. A Government agent cannot be a co-conspirator in this context, a fact acknowledged by the Government in it not listing any of its agents as co-conspirators in its Bill of Particulars definitively listing conspirators.[83]

[80] *Fortenberry*, 92 F.4th at 1135–36.

[81] 18 U.S.C. § 1956(h); *Whitfield v. U.S.*, 543 U.S. 209, 214 (2005).

[82] 18 U.S.C. § 1956(i); *Whitfield* at 214.

[83] *See, e.g.*, *U.S. v. Nunez*, 889 F.2d 1564, 1569 (6th Cir. 1989); A. 6832.

The District Court also erred by instructing the jury that an overt act by a Government agent could establish venue for a conspiracy as to Count One.[84] The Indictment only alleges the Government mixed Bitcoin in Count Two. But this cannot serve as the basis for venue for Count One, as the Government must show proper venue for each count.[85] An agent's conduct, as alleged in Count Two cannot supply the overt act for Count One where no Government conduct is mentioned. Under § 1956(i), the Government must prove that the conspiracy to money launder, or an act in its furtherance, occurred by Sterlingov or a co-conspirator in D.C. In essence, the District Court allowed the jury to find venue on Count One via conduct only alleged in Count Two.[86]

Speculative digital traces and attributions alone are insufficient to establish venue for a conspiracy. Particularly when the tracing software, Reactor, is incapable of making geographical tracing attributions as part of its output. In *Mackey*, the Second Circuit reversed a conspiracy conviction under 18 U.S.C. § 241 because nothing in the record established that the defendant viewed or participated in private

[84] A. 6288-89.

[85] *See, e.g., Auernheimer***,** 748 F.3d at 535.

[86] A. 6561.

group exchanges where the conspiracy was formed.[87] The court concluded that the Government failed to prove that Mackey knowingly agreed to join the charged conspiracy. So too here: the Government's case relies on circumstantial inferences and speculation about anonymous internet activity, none of which is tied to D.C. or establishes a knowing agreement. As with Count Two, the Government's theory reads *mens rea* out of the statute. Such speculation cannot support a conspiracy conviction, let alone confer venue.

Because there is no evidence that Sterlingov, or any co-conspirator, agreed, communicated, acted in, or directed activity towards, D.C., venue for Count One is unconstitutional.

2. Venue is Unconstitutional for Count Two Because there was No Communicated Representation and the Mixed Bitcoin was Licit

Count Two of the Superseding Indictment charges Sterlingov under 18 U.S.C. § 1956(a)(3)(B), based on the mixing of roughly $86 of Bitcoin by a Government agent sitting at a computer in D.C. [88]

IRS-CI Price testified that in 2019 he deposited Government Bitcoin into a Government-operated Apollon market account.[89] Price did not testify that they were

[87] *See U.S. v. Mackey*, 143 F.4th 129, 140-46 (2d Cir. 2025).

[88] A. 6561.

[89] A. 2857-72.

criminal proceeds. He then sent a message to Bitcoin Fog's help-desk claiming he wanted to launder drug money.[90] The message received no response, and there is no evidence it was received or that anyone ever saw it.[91] There is no evidence that the Bitcoin Fog help desk was even operational at the time. Price then mixed the Bitcoin from the Apollon account through Bitcoin Fog.[92]

The mere fact that Government Bitcoin was sent to Bitcoin Fog from the Government's own Apollon account does not establish that the funds were illicit. Nor is there any evidence Bitcoin Fog had any way of knowing that the address it was receiving Bitcoin funds from was Apollon's, given the that the blockchain doesn't record that type of information. Bitcoin merely being in a darknet account does not make illicit. Later testimony at trial established that darknet markets also sell legal goods like books, and Price appears to have used the Government Apollon account simply as a wallet.[93]

Price's message cannot constitute a representation for purposes of 18 U.S.C § 1956(a)(3) because there is no evidence that anyone ever saw it. [94] The Government

[90] *Id.*

[91] A. 3038. (Price testifying the message received no response).

[92] A. 3037-38.

[93] A. 5232; A. 3037-38.

[94] A. 3038.

cannot satisfy the statute's *actus reus* or *mens rea* requirements with its own unacknowledged unilateral conduct. Indeed, the recent DOJ Blanche Memo reinforces this by stating the Government will no longer prosecute mixer operators for the crimes of their end-users.[95]

Here, the Government's use of licit Bitcoin, and the fact that there is no evidence Price's message was seen by anyone, not only establishes that venue is improper but that no substantive crime occurred. Allowing venue to rest solely on the Government's single, unrequited message and the mixing of licit Bitcoin would allow prosecutors to fabricate venue in any district at will by logging in, typing a message, and clicking send. Under the Government's theory, § 1956(a)(3) becomes a strict liability statute. This explains why the Government sought, and received over objection, a willful blindness jury instruction. Not only is the Government manufacturing venue here, it is manufacturing *mens rea*.

3. Venue is Unconstitutional for Count Three Because There was no Business Conduct in D.C.

18 U.S.C. § 1960(a) requires that the defendant must have "conducted, controlled, managed, supervised, directed, or owned all or part of an unlicensed money transmitting business." But the Government introduced no evidence that

[95] A. 7217-20.

Sterlingov, or any alleged co-conspirator, operated such a business in D.C. There is no evidence that Sterlingov or co-conspirators advertised, held accounts, directed policies, or interacted with users in the District. There is no evidence of any users in D.C. besides the Government's three mixes.

The Government's venue theory is astonishingly broad. It maintains that accessing an internet site anywhere in the world from D.C. constitutes doing business in D.C. The fact that Bitcoin Fog was accessible from D.C. is not sufficient to establish venue. Courts distinguish between passive website availability and affirmative business operations directed at a forum. Evidence of targeted commercial conduct, such as local advertising or solicitation is required.[96] At all relevant times, Sterlingov was in Sweden, except for his 2017 Miami trip where the Government put him under surveillance, but neither arrested him, nor produced anything from this trip at trial.[97] Three Government mixes from this District over three years, in the context of a Government investigation covering a decade, does not constitute Bitcoin Fog conducting business in D.C.

[96] *See*, *e.g., GTE New Media Servs. Inc. v. BellSouth Corp.*, 199 F.3d 1343, 1349 (D.C. Cir. 2000); *Triple Up Ltd. v. Youku Tudou Inc.*, No. 17-7033, 2018 WL 4440459, at *2 (D.C. Cir. July 17, 2018); *Forras v. Rauf*, 812 F.3d 1102, 1106 (D.C. Cir. 2016); *Bensusan Restaurant Corp. v. King*, 126 F.3d 25, 29 (2d Cir. 1997).

[97] A. 3031-32.

4. Venue is Unconstitutional on Count Four Because Bitcoin Fog Did Not Operate from D.C.

D.C. Code § 26-1001(10) defines "money transmission" to include "engaging in the business of receiving money for transmission or transmitting money within the U.S., or to locations abroad." The statute thus contemplates an entity actively operating a money-transmitting business within the District**.** Under any reasonable reading of the statute and the evidence, a rational jury could not conclude that venue was proper in D.C. on Count Four.

As with all counts, there is no evidence that Bitcoin Fog operated from within this District. D.C. Code § 26-1001 plainly requires an operational presence in D.C., namely, receiving or sending money in D.C., or operating a money-transmitting business from D.C. to abroad. To read it otherwise would grant the D.C. municipality universal jurisdiction over any money-transmission service accessible via the internet anywhere in the world.

II. The Government's Blockchain and IP Attribution Evidence Fails *Daubert*

The District Court erred by admitting expert testimony based on Chainalysis Reactor and a novel IP address overlap analysis, neither of which satisfied the reliability requirements of Fed. R. Evid. 702 or *Daubert*. Chainalysis Reactor failed to meet any of the four Daubert factors. Its methodology was opaque, untestable, and undisclosed. It had no known error rate, peer-reviewed validation, or scientific acceptance. The Government relied instead on anecdotal affirmations from law enforcement users, which courts have repeatedly deemed insufficient to establish reliability. Without access to the proprietary software's source code, off-chain data, or internal heuristics, neither the Defense nor the court could meaningfully evaluate the tool's accuracy.

The Government's IP address attribution evidence was similarly flawed. It rested on an untested, one-off overlap method developed for this case by an analyst who admitted it had never been used before, could not be tested, and lacked peer-review. As with Reactor, the Government presented no scientific validation for this method. By admitting expert conclusions drawn from secret algorithms and unvalidated techniques, the District Court abdicated its gatekeeping role under *Daubert*, and allowed unreliable evidence to go to the jury. This evidentiary error severely prejudiced Sterlingov and warrants reversal.

A. Standard of Review

A district court's determinations of reliability under a proper application of *Daubert* are reviewed for abuse of discretion.[98] But where, as here, the District Court

[98] *See, Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579 (1993); *U.S. v. Day*, 524 F.3d 1361 (D.C. Cir. 2008).

incorrectly applied the *Daubert* factors and the requirements of Fed. R. Evid. 702, and failed to perform its gatekeeping role, the standard of review is *de novo*.[99]

B. Chainalysis Reactor Fails to Satisfy Any Daubert Factor of Reliability

The Government's expert witnesses, Luke Scholl of the FBI, and Elisabeth Bisbee from Chainalysis Government Solutions, both testified to using proprietary Chainalysis Reactor software to formulate their opinions on the flow of Bitcoin through the blockchain to and from (but not through) Bitcoin Fog. Bisbee specifically testified that neither her nor Reactor made any attribution as to Sterlingov operating Bitcoin Fog.[100]

Chainalysis Reactor probabilistically clusters Bitcoin addresses assumed to be controlled by the same entity and then attributes those clusters to particular entities.[101] In this case, Reactor clustered and attributed to Bitcoin Fog over 925,743 Bitcoin addresses, traced receipt of approximately 1,284,251 Bitcoin valued at almost $400 million to Bitcoin Fog, and traced withdrawals of approximately 1,280,935 Bitcoin from Bitcoin Fog.[102] The software also linked Bitcoin Fog to

[99] *U.S. v. Nacchio*, 555 F.3d 1234, 1241 (10th Cir. 2009) (*en banc*).

[100] *See, e.g.,* A. 608.

[101] *See, e.g.,* A. 6951.

[102] *Id.*

marketplaces on the private Tor network, concluding that eight such markets sent an aggregate of about 80,729 Bitcoin to Bitcoin Fog and received over 45,152 Bitcoin from Bitcoin Fog.[103]

For these clustering outputs, Chainalysis Reactor employed three heuristics. Heuristic 1 was a co-spend heuristic based on the assumption that when multiple Bitcoin addresses fund a single transaction, the sender likely controls all input addresses.[104] Heuristic 2 was a behavioral clustering heuristic that analyzed unique patterns and behaviors by entities in Bitcoin transactions.[105] Heuristic 3 was an intelligence-based attribution derived from "other sources" of data exogenous to the publicly visible blockchain, such as "data leaks, court documents, Chainalysis data partnerships," and information shared by cryptocurrency exchanges.[106] Chainalysis's database containing such off-chain data remains proprietary and secret.[107]

[103] A. 6951; A. 6465; A. 6400; A. 6951.

[104] A. 6951; A. 6465; A. 6400; A. 6465; A. 6473.

[105] *See, e.g.,* A. 6951.

[106] A. 6964; A. 6474.

[107] *See e.g.,* A. 6860; A. 6877; A. 6884; A. 6888; A. 6901; A. 6912; A. 6930.

Accordingly, Sterlingov challenged the admissibility of the Chainalysis Reactor evidence and related expert testimony as unreliable under Fed. R. Evid. 702, arguing it failed to meet any of the *Daubert* factors.[108] The Defense argued that the lack of any peer-review or independent testing of the Chainalysis Reactor software, and the complete lack of any known error rates, false positive rates or false negative rates showed the software was unreliable under *Daubert*.

The District Court rejected these arguments, finding it "more likely than not" that the evidence was "the product of reliable principles and methods."[109] The court was persuaded by anecdotal testimony from the Government's witnesses about Reactor's reliability. Scholl testified that in his experience using Reactor since 2016, he could not recall an instance "where [the] Chainalysis attribution wasn't correct" when verified through subpoenas to cryptocurrency exchanges.[110] Bisbee of Chainalysis testified that in her work at the DEA and Chainalysis spanning hundreds of investigations involving thousands of addresses, she was not aware of a single false positive.[111]

[108] *See, e.g.,* A 503-656; A. 1356-1409.

[109] A. 6951.

[110] A. 6971-72.

[111] A. 6972.

The District Court found that Reactor's reliability was further corroborated by the Government’s spot testing of the software. The FBI and IRS used Bitcoin Fog and attributed five Bitcoin addresses to Bitcoin Fog.[112] Chainalysis Reactor, however, had correctly attributed only four of those five addresses to Bitcoin Fog (a 20% discrepancy).[113] Additionally, the court found significant that Sterlingov had previously testified to using Bitcoin Fog (but not operating it), which the court characterized as conceding "the very thing that the Government was trying to prove through its blockchain analysis."[114] But this individual usage of the Bitcoin Fog service doesn’t amount to verification of Reactor’s reliability.

While acknowledging that Reactor had not itself been subject to peer review, the court noted that the theory behind Heuristic 1 (the co-spend heuristic) has received academic approval, with its origins in the white paper that invented Bitcoin.[115] The court further held that Chainalysis does not gather and record an error rate "in a central location," but found this did not undermine Reactor's reliability

[112] A. 6408-10.

[113] A. 6972-82.

[114] *Id.*

[115] *Id.*

given the other evidence.[116] There is no evidence in the record of Chainalysis ever doing any error rate analysis, and Bisbee testified as such.[117]

The court ultimately concluded that "blockchain analytics in general, and Reactor in particular, is not junk science" and that the Government's blockchain tracing evidence "readily clears the hurdle necessary to reach the jury."[118] The court thus denied Sterlingov’s requests to exclude testimony and evidence based on Chainalysis Reactor.[119]

The Supreme Court in *Daubert* explained that Fed. R. Evid. 702 guides the analysis for the admission of expert testimony.[120] Fed. R. Evid. 702 provides a list of guidelines for admitting expert testimony:

> A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if: (a) the expert’s scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue; (b) the testimony is based on sufficient facts or data; (c) the testimony is the product of reliable principles and methods; and (d) the expert has

[116] *Id.*

[117] *See, e.g.,* A. 619; A. 639-40; *see also* A. 622-23; A. 627-28.

[118] A. 6972-82.

[119] *Id.*

[120] *Daubert v. Merrell Dow Pharms, Inc.,* 509 U.S. 579, 594 (1993).

> reliably applied the principles and methods to the facts of
> the case.[121]

Pertinent here, Rule 702 requires that the expert witness's testimony be the product of "reliable principles and methods."[122] *Daubert* instructs that for the trial court to discharge its duty as the "gatekeeper" of scientific or specialized expert evidence, it should examine:

1. whether the theory or technique can be, and has been, *tested*.
2. whether the theory or technique has been subjected to *peer review* and *publication*
3. in the case of a particular scientific technique, the court ordinarily should consider the known or potential *rate of error*, and
4. general acceptance of a relevant *scientific community*[123]

This gatekeeping function "inherently require[s] the trial court to conduct an exacting analysis" of the foundations of expert opinions to ensure they meet the standards for admissibility under Rule 702.[124]

[121] Fed. R. Evid. 702.

[122] *Id.*

[123] *See*, *Daubert* 509 U.S. at 592-94 (*emphasis added*).

[124] *U.S. v. Frazier*, 387 F.3d 1244, 1260 (11th Cir. 2004).

Moreover, as reiterated by the 2023 amendments to Rule 702, "the proponent [must] demonstrate [] to the court that it is more likely than not that" the four *Daubert* guidelines are satisfied.[125]

C. The District Court Erred in Accepting Unverified, Untestable, Non-Peer-Reviewed Evidence

The Government conceded that there is no known error rate for the Reactor software, a fact the District Court also openly acknowledged in its order denying Sterlingov's *Daubert* challenge.[126]

To overcome this conspicuous gap in the reliability analysis, the Government offered, and the court erroneously accepted, the anecdotal testimony of Reactor's end-users.[127] Such anecdotal case reports "are universally regarded as an insufficient scientific basis for a conclusion" because they inherently "lack controls."[128] "Uncontrolled anecdotal information," like that supplied by the Government here to

[125] Fed. R. Evid. 702 (2023); *see also,* Fed. R. Evid. 702, Notes of Advisory Cmt. on 2000 amend.; *see also Bourjaily v. U.S.*, 483 U.S. 171 (1987).

[126] A. 6979.

[127] *See,* A. 6970-71.

[128] *Allison v. McGhan Med. Corp.*, 184 F.3d 1300, 1316 (11th Cir. 1999) (quoting *Hall v. Baxter Healthcare Corp.*, 947 F. Supp. 1387, 1411 (D. Or. 1996) (collecting cases)).

establish Reactor's reliability, offers "one of the least reliable sources to justify opinions" and is not one of the factors enumerated in *Daubert* or Rule 702.[129]

Nor could the uncontrolled anecdotal evidence possibly substitute for a *Daubert* analysis of independently controlled testing and peer review of the Chainalysis Reactor software.[130] The District Court found that the Reactor software was testable because the underlying blockchain data is public.[131] But this logic conflates the ability to test the publicly available inputs with the ability to test the proprietary process by which Reactor produced its conclusions. Heuristics 2 and 3 were based on algorithms that – to use a metaphor – weighed multiple factors, as well as rafts of off-chain data, held in Chainalysis's proprietary databases. Without complete access to the proprietary heuristics, source code, the specific algorithmic parameters, and the off-chain data-sets used to create the attributions and conclusions, an outside party could not truly test the method itself, they could only compare the output to results from their own, different methods. The Government

[129] *McClain v. Metabolife Int'l, Inc.*, 401 F.3d 1233, 1250 (11th Cir. 2005).
[130] *Daubert v. Merrell Dow Pharms, Inc.,* 509 U.S. 579, 593-94 (1993).
[131] A. 6951.

offered limited testimony on the internal workings of the program and refused to produce the source code or outside datasets used.[132]

At the pretrial *Daubert* hearings, Appellant's *Daubert* witness on blockchain forensics, Jonelle Still from the company Ciphertrace (a subsidiary of MasterCard), used her company's blockchain forensics tool and obtained different attribution results from those produced by Chainalysis Reactor.[133] Rather than the 925,743 addresses Chainalysis Reactor attributed to the Bitcoin Fog cluster, Ciphertrace's software attributed only 398,011.[134] In other words, Reactor's attributions to Bitcoin Fog were over-inclusive, when compared with Ciphertrace's software, by including 527,731 addresses that were likely not involved with Bitcoin Fog at all.

Moreover, when comparing the two-software program's Tor-network marketplace attributions, there were discrepancies in 9 of the 11 marketplace clusters, with rates of discrepancy ranging between 96% and 1%.[135] Still explained

[132] *See, e.g.,* A. 6860; A. 6884.

[133] A. 6761-6831. Ciphertrace pulled the testimony of its employee Jonelle Still out of fear of being sued by Chainalysis and for undisclosed reliability reasons. Nonetheless, the District Court, in its *Daubert* Opinion, relied on Still's expert report knowing this fact. A. 6951.

[134] A. 6792; A. 6474.

[135] A. 6799.

that these discrepancies between the two companies' programs (including the inclusion of 527,731 additional addresses in the Bitcoin Fog cluster) stemmed from Chainalysis's use of Heuristics 2 (behavioral) and 3 (off-chain intelligence data), which heuristics Ciphertrace eschews as "unreliable and not a true representation of the flow of funds on chain."[136] Still also attributed the discrepancies to "other unnamed heuristics utilized by Chainalysis, which were not explicitly stated in their expert reports."[137]

Still's testing on a separate software program, while not a controlled test by independent auditors in accordance with *Daubert*, indicates serious shortcomings in Chainalysis' Reactor software that warrant rigorous examination, and which shortcomings the Government failed to address, choosing rather to fight access to the software by Sterlingov.

Despite Reactor's over-inclusion of 527,731 addresses, Reactor failed to attribute one of the five addresses in one of the Government's mixes to Bitcoin Fog (none of which Reactor attributed to Sterlingov).[138] Scholl concluded that this

[136] A. 6764.

[137] *Id.*

[138] A. 6411.

unattributed address should have been flagged as part of Bitcoin Fog, as it was "logical that [the unattributed address] would have received funds from other Bitcoin Fog addresses based on the necessary behavior of a Bitcoin mixer."[139] That is, by not attributing the address, Reactor's attribution output was illogical. Reactor erred. But the Government offered no explanation for this.

The District Court accepted the Government's suggestion that *Daubert's* peer-review inquiry was satisfied by a single non-peer-reviewed whitepaper that pre-dated Reactor and only discussed the theory underlying co-spend heuristic (Heuristic 1).[140] This falls far short. First, the article only addressed Heuristic 1. And the paper discussed this single type of heuristic generally but did not examine Reactor's particular use of the heuristic. The correct inquiry under *Daubert* is whether the forensic method has been tested and the results peer reviewed, not whether the background theory behind the method has been discussed in journals. It is the difference between a scientific empirical approach as *Daubert* counsels and unverified *a priori* reasoning. The difference between theory and practice. Indeed, "*Daubert* applies not only to testimony about scientific concepts but also to

[139] *Id.*

[140] A. 6951.

testimony about the actual applications of those concepts."[141] Peer review is "critical to 'good science' since 'it increases the likelihood that substantive flaws in methodology will be detected.'"[142]

The District Court's approach of substituting biased law enforcement anecdotal evidence for (i) controlled testing, (ii) peer review, and (iii) known error rates, contrasts with courts that undertake a truly "far-reaching and searching inquiry" into the reliability of novel forensic software.[143]

In *Gissantaner*, for example, the Sixth Circuit meticulously evaluated STRMix, a probabilistic DNA analysis software, against each *Daubert* factor, finding the technology satisfied all reliability requirements.[144] STRMix had been subjected to (i) systematic laboratory testing using controlled mixtures with known contributors; (ii) extensive peer review evidenced by over fifty published articles; (iii) had quantifiable error rates demonstrating 99.1% accuracy in excluding non-contributors; and (iv) was widely accepted across forty-five forensic laboratories.[145]

[141] *U.S. v. Lee,* 25 F.3d 997, 999 (11th Cir. 1994).

[142] *U.S. v. Harris*, 502 F. Supp. 3d 28, 39 (D.D.C. 2020) (quoting *Daubert*, 509 U.S. at 593–94).

[143] *State v. Chun*, 194 N.J. 54, 148 (2008).

[144] *U.S. v. Gissantaner*, 990 F.3d 457 (6th Cir. 2021).

[145] *Id*. at 464-69.

This extensive scientific track record demonstrated that STRMix was "the product of reliable principles and methods."[146]

Reactor can boast of no such track record. The District Court here admitted Chainalysis Reactor evidence despite the Government's concession that the software possessed no known error rates, no peer-reviewed validation, and no controlled testing methodology — relying instead solely on biased law enforcement anecdotal post-hoc verification.

But even without having been subjected to the level of scientific study that STRMix has, a novel forensic software may nonetheless still be deemed reliable if properly examined. In *Chun*, for example, a special master engaged in a lengthy process of receiving evidence on a breathalyzer tool and, crucially, "directed that the manufacturer divulge its source code and make available the personnel who can explain it."[147] Only after permitting this exhaustive evaluation of the source code did the court become "confident that its errors have been revealed."[148]

[146] *Id*. at 466 (quoting Rule 702).

[147] *Chun*, 194 N.J. at 148.

[148] *Id*. at 131–32.

Such errors, for example, can take the form of accidental coding errors in Reactor. A study conducted on C++ developers found that "33% of highly experienced programmers failed to correctly use parentheses when coding basic equations, resulting 'in almost 1% of all expressions contained in source code being wrong.'"[149] Examination of the source code would also have revealed how Reactor's algorithms function: *i.e.*, with what thresholds the heuristics are applied, as well as how the intelligence data from Heuristic 3 was weighted.

Because "software is not immune from error," "independent source-code review is critical when determining reliability."[150] In *Pickett*, the New Jersey Superior Court appellate division reversed an order denying a criminal defendant access to the underlying source code of another probabilistic DNA genotyping software called TrueAllele, which the defendant had sought to challenge the software's reliability and admissibility.[151] In granting access to the source code, the court reasoned that "[e]ven if the DNA science underpinning probabilistic genotyping analysis has been proven scientifically valid, computer software such as

[149] Christian Chessman, "A 'Source' of Error: Computer Code, Criminal Defendants, and the Constitution," 105 Cal. L. Rev. 179, 186-89 (2017).

[150] *State v. Pickett*, 256 A.3d 279, 284 (Super. Ct. App. Div. 2021).

[151] *Id*.

TrueAllele must also properly implement that analysis in its source code; the source code must do as Cybergenetics says it does."[152]

Likewise, Reactor must properly implement any scientifically valid heuristics in its source code (not to mention any untested, proprietary heuristics) and that code must do as Chainalysis says it does. "Fundamental due process and fairness demand access."[153]

To be sure, access to the source code may be appropriately conditioned on defense experts agreeing to an "appropriate protective order" — one that is not unduly restrictive or deterring.[154] Overly restrictive orders that take the form of aggressive non-competition agreements – as happened here – do not fit the bill.[155] For that reason, the court in *Pickett* criticized the proposed non-disclosure agreement.[156] Under that non-disclosure agreement, the defense's expert would have been "bound to accept responsibility for any legal and financial consequences,

[152] *Id*. at 307.

[153] *Id*. at 284.

[154] *Id*. at 301.

[155] A. 6860.

[156] *State v. Pickett*, 246 A.3d 279, 289 (Super. Ct. App. Div. 2021).

including a $1,000,000 automatic fine, in the event of a breach."[157] "A provision that no "expert would agree to."[158] The court directed on remand that such draconian provisions be removed in favor of standard language that review of the source code was restricted to purposes of the case, and that parties who violate the order could be subject to civil or criminal sanctions.[159]

Here, the Defense and their experts were asked to sign the following non-compete clause in a new proposed protective order:

> I further swear and affirm that I am not a past or current employee of a competitor to Chainalysis, that I am not and am not anticipated to become an employee of a competitor to Chainalysis, that I am hereby prohibited from engaging in competitive behavior with Chainalysis during this litigation and for five years following the conclusion of this litigation.[160]

Such draconian non-competition provisions deterred Defendant's own experts from reviewing Chainalysis's heuristics.[161] Trial Defense Counsel refused to sign the non-competition protective order. Proposed defense expert witnesses Laurent

[157] *Id*. at 290.

[158] *Id*.

[159] *Id*. at 309.

[160] A. 6868.

[161] A. 6860.

Salat, founder of blockchain tracing firm OXT, and Bryan Bishop, a well-known Bitcoin Core developer, refused to sign it as well. Because of Chainalysis' aggressive non-compete clause and assertion of its intellectual property rights, Sterlingov's blockchain tracing expert, Jonelle Still of Ciphertrace, ultimately refused to review Chainalysis' limited heuristic production due to concerns that this could expose her and Ciphertrace to claims of misappropriating Chainalysis's proprietary heuristics; ultimately Ciphertrace forbid her from testifying on Sterlingov's behalf.[162] Ciphertrace was independently working on a similar heuristic model.[163]

Finally, the Government's argument and the District Court's finding on the "general acceptance" *Daubert* factor misses the mark. The District Court was persuaded by Reactor's widespread adoption by law enforcement and financial institutions.[164] But this mistakes *market acceptance* for *scientific acceptance*. *Daubert* requires acceptance by the "relevant scientific community," not the community of users and purchasers.[165] Crediting market share creates a self-

[162] A. 6888.

[163] A. 6912.

[164] A. 6980.

[165] *Daubert v. Merrell Dow Pharms, Inc.,* 509 U.S. 579, 594 (1993).

reinforcing loop where Government procurement decisions and a company's sales success become proxies for independent scientific validation, subverting the core purpose of the *Daubert* inquiry and inserting a profit motive into forensic analysis.

Chainalysis Reactor failed to satisfy any of *Daubert*'s four factors. Without the ability to examine its source code and other proprietary inputs, there was no way to verify its reliability. Sterlingov's *Daubert* motions should have been granted and the Government's Reactor evidence and expert opinions based on it excluded.

D. The Novel IP Address Overlap Technique Lacked Any Indicia of Reliability under *Daubert*

At trial, the only evidence linking Defendant to the Bitcoin Fog operation was a so-called IP Overlap Analysis performed by the Government expert Valerie Mazars de Mazarin.[166] Mazars conceded that when she performed a search of all of Sterlingov's devices, she found no private keys to any of the Bitcoin Fog cluster addresses, no administrator passwords to Bitcoin Fog, no log-in credentials to Bitcoin Fog servers, and, in fact, "Bitcoin Fog" appeared nowhere within any of his

[166] A. 6532; A. 6539.

devices.[167] Nor did Mazars find any communications between Sterlingov and any pseudonymous operator or operators of Bitcoin Fog.[168]

Mazars linked the Appellant to Bitcoin Fog by using a speculative "IP Overlap Analysis" that she made up for purposes of this case, had never performed before, and could cite no scientific basis for nor any error rates.[169] In a convoluted report, she examined timestamps (not from original logs as she did not have them) and the alleged ownership of internet accounts, then applied subjective "overlap windows" (ranging from 10 minutes to 12 months) to infer possible shared use of IPs by different accounts.[170] IP addresses do not identify individual ownership and can be shared by countless users.[171] Mazars made no definitive attribution that Sterlingov controlled accounts affiliated with the operation of Bitcoin Fog.[172]

As for the exact methodology behind her analysis, Mazars conceded it was her IP overlap analysis was unique to this case.[173] It was a freshly designed analysis

[167] A. 4840-41.

[168] A. 4844-45.

[169] A. 4853-55; A. 4857.

[170] A. 6532; A. 6539.

[171] A. 4846-50.

[172] A. 1397.

[173] A. 4853.

bespoke to the dataset she was given in this case. Mazars considered this a "research analysis," not a scientific analysis, and thus there were no peer-reviewed papers attesting to the accuracy or reliability of her methodology.[174] She admitted the method she used "couldn't be tested."[175]

Indeed, the reliability of this simplistic timing overlap method is suspect. Mazars admitted that hundreds, if not thousands, of people could be sharing the same IP address. Mazars testified that individuals could be connected on the same location's Wi-Fi internet (a daily occurrence for every Starbucks in the world), be using the same VPN provider or be, using the same proxy server – all daily occurrences.[176] Many people access many different accounts close in time to one-another, despite, of course, being unconnected individuals. Moreover, the time-stamp excerpts (Mazars testified she did not have access to original logs) she reviewed did not state the time zone being used, and thus she was inferring what the

[174] A. 4854.

[175] *Id.*

[176] A. 4847.

time was.[177] The actual temporal smoking gun could have been off by hours, days, months, or years.[178]

E. Mazars' Testimony is Unreliable Under *Daubert*

Mazars' report is the main piece of evidence linking Sterlingov to Bitcoin Fog. Without it, the Government's case lacks foundation. As a witness with "specialized knowledge" and expertise offering an opinion or conclusion based on a methodological analysis of facts, Mazars' testimony was the proper subject of a *Daubert* challenge.[179] As she readily admitted, her IP address temporal overlap methodology was novel, performed for the first time during this investigation, untestable, without any peer review, and, because she created it for this specific investigation, not accepted in any computer science community. Certainly, the Government put on no evidence to support the *Daubert* factors and secure the admissibility of Mazars' testimony. This evidence was prejudicial and should have been excluded.

[177] A. 6532.

[178] A. 4851-52.

[179] *Daubert v. Merrell Dow Pharms, Inc.,* 509 U.S. 579, 589 (1993).

III. The Government's Use of Closed Source Software Violated Sterlingov's Sixth Amendment and Due Process Rights.

A. Standard of Review

This Court's "review of the district court's legal conclusions regarding the Confrontation Clause is *de novo*, and subject to constitutional harmless error analysis."[180] Where an error under the Confrontation Clause has occurred, a court will reverse unless the Government can establish that "the error was harmless beyond a reasonable doubt."[181]

B. Admitting Testimonial Assertions from Reactor Software Violated Sterlingov's Sixth Amendment Rights

The Government presented the testimony of experts who formulated their reports and conclusions by directly relying on conclusions that were the output of the closed-source, proprietary blockchain tracing software Chainalysis Reactor. Reactor clustered Bitcoin addresses together based on heuristics, and then attributed those clusters to specific entities such as Bitcoin exchanges, online marketplaces on the private Tor network, and Bitcoin Fog itself. These attributions were based on heuristics that included undisclosed inputs of data from various sources outside the

[180] *U.S. v. Moore*, 651 F.3d 30, 69 (2011).

[181] *Id*. at 74.

Bitcoin blockchain, as well as behavioral characteristics.[182] The Government's experts accepted those clustering attributions by Reactor wholesale; they did not make the attributions themselves. In other words, Reactor computed forensic conclusions that were subsequently relied upon by the Government's experts in forming their conclusions.

But Sterlingov was denied full access to Reactor.[183] He attempted to examine the basis for Reactor's conclusions by requesting access to Reactor's source code, among other things, to determine how the clustering conclusions operated, which the District Court denied.[184] And, although some of the heuristics behind the conclusions were disclosed to Defense counsel in limited fashion, without the external intelligence data which Reactor relied upon, the information was of limited use. Exacerbating the issue, Sterlingov himself was barred from seeing this evidence.[185]

This use of heuristic algorithmic conclusions in the Government's experts' reports, and at trial, without affording Sterlingov the opportunity to examine the

[182] *See e.g.* A. 6465-92; A. 5093 *et. seq.*; A. 6761 *et. seq*.

[183] A. 6912-29.

[184] *Id.*

[185] A. 6912; A. 6930-41.

assumptions and reasoning behind those conclusions, violated his Sixth Amendment right to confront witnesses.

The Confrontation Clause mandates that in all criminal prosecutions the accused has the right "to be confronted with the witnesses against him."[186] Testimonial statements by non-testifying witnesses are inadmissible unless the witness is unavailable and the defendant had a prior opportunity for cross-examination.[187]

Reactor is a specific "investigative tool" used primarily for law enforcement purposes, sold on a subscription basis, by Chainalysis Government Solutions.[188] "A document created solely for an 'evidentiary purpose,'… made in aid of a police investigation, ranks as testimonial."[189] The attribution outputs of Reactor, which are "made in aid of [government] investigation[s]," therefore, "rank[] as testimonial."[190]

[186] *See, e.g.*, U.S. Const. Am. VI; *Melendez-Diaz v. Mass.*, 557 U.S. 305, 309 (2009).

[187] *Ohio v. Clark*, 576 U.S. 237 (2015); *Crawford v. Wash.*, 541 U.S. 36 (2004).

[188] *See, e.g.,* A. 621.

[189] *Bullcoming v. New Mexico*, 564 U.S. 647, 664 (2011). (quoting *Melendez-Diaz* 557 U.S. at 311).

[190] *Id.* at 664; *see also, U.S. v. Cameron*, 699 F.3d 621, 643 (1st Cir. 2012) (analyzing whether reports had the "primary purpose of establishing or proving past events potentially relevant to a later criminal prosecution.") (quoting and applying *Bullcoming*, 564 U.S. at 659 n.6).

Indeed, the "central concern of the Confrontation Clause is to ensure the reliability of the evidence against a criminal defendant by subjecting it to rigorous testing in the context of an adversary proceeding before the trier of fact."[191] The Confrontation Clause guards against the use of "unconfrontable but impressive-looking" evidence that denies a defendant the ability to test the basis of an accusation.[192] Denying confrontation for machine-generated evidence, like Reactor's clustering attributions, that is presented with a veneer of scientific neutrality "resembles trial by ex parte affidavit."[193]

Although machine-generated, Reactor's attribution outputs are the product of algorithms programmed by humans (the Chainalysis software developers and data scientists) who made judgments how to encode the heuristics, what intelligence and data existing outside the blockchain to include, and how to give weight to that off-chain data. Such human design choices give programmers "subjective control over decisions like threshold values."[194] Moreover, they can lead a machine to produce false or misleading information where the programmer makes inappropriate

[191] *Maryland v. Craig*, 497 U.S. 836, 845 (1990).

[192] Benjamin Welton, *Meaningful Machine Confrontation*, 76 STAN. L. REV. 845, 858 (2024).

[193] *Id.*

[194] *Id.* at 870.

analytical assumptions or omissions, mistakes, or where a programmer's conscious or unconscious bias influences an algorithm's predictions.[195] AI hallucinations are an example of this. In fact, Scholl testified that different blockchain tracing software will "often have different attributions," or "one will have an attribution and one won't have an attribution," and "it's possible that those platforms disagree."[196]

Thus, a Reactor attribution linking a Bitcoin address to a Tor network market based on behavioral patterns, for example, is not an objective, observable fact of the blockchain; rather, it is an inference drawn from a proprietary, human-designed model. Reactor is not a mere measurement tool mechanically outputting data about the observable world, like a bathroom scale. It is the product of human decisions and judgments, like a forensic lab analyst testing their conclusion. Thus, its attributions and analyses are testimonial.

Reactor algorithmically claimed that 925,743 individual Bitcoin addresses belonged to the Bitcoin Fog cluster; that hundreds of thousands of other Bitcoin addresses belonged to various Tor network online marketplaces; and still more addresses belonged to specific Bitcoin exchanges and wallets.[197] The Government's

[195] *See,* Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 1995–96 (2017).
[196] A. 4142.
[197] A. 6465-92.

experts included those algorithmic declarations in their own reports, assuming them to be true and without which the experts could not formulate their opinions.[198]

Accordingly, the Government's experts were "mere scrivener[s]" who wrote down and reported the Reactor analyses on clustering.[199] The experts should not have been qualified because of this. The Supreme Court has consistently maintained that the "Confrontation Clause may not be 'evaded by having a note-taking police officer recite the . . . testimony of the declarant.'"[200] In *Bullcoming*, the Court explained that the testifying forensic expert, who had not performed the forensic tests, "could not convey what [the non-testifying analyst] knew or observed about the events his certification concerned, *i.e.*, the particular test and testing process he employed."[201] Thus, because the defendant there could not examine the process by which the forensic conclusions were derived, the Confrontation Clause was violated.

Likewise, here, Sterlingov was afforded no meaningful opportunity to examine the heuristics, algorithmic processes, source code, and datasets by which Reactor's forensic analyses about entity clusters and the relationship between those

[198] *See, Smith v. Arizona*, 602 U.S. 779, 783 (2024).

[199] *Bullcoming v. New Mexico*, 564 U.S. 647, 672 (2011) (Sotomayor, J., concurring) (quoting *State v. Bullcoming*, 226 P.3d 1, 9 (N.M. 2010)).

[200] *Id*. at 660 (quoting *Davis v. Washington*, 547 U.S. 813, 826, (2006)).

[201] *Bullcoming*, 564 U.S. at 661.

clusters was created. With human forensic analysts, the examination has traditionally taken the form of cross-examination. But algorithmic analysis like Reactor can only be confronted through an examination of their source code, heuristics, external inputs, and the weighting given to any such external inputs within the algorithms. Thus, Sterlingov was denied the ability to confront this machine-generated testimony parroted by the Government's human expert witnesses. This violates the Confrontation Clause.

The Government argued, and the District Court ruled, that good cause under Fed. R. Crim P. 16 required the non-disclosure of the requested Reactor discovery.[202] Under Rule 16, discovery may be precluded if necessitated by "the safety of witnesses and others, a particular danger of perjury or witness intimidation, the protection of information vital to the national security, and the protection of business enterprises from economic reprisals."[203] But Sterlingov was not a competitor of Chainalysis in the marketplace and thus there was no risk of an economic reprisal. Nor was there any allegation of perjury, witness intimidation, or witness safety.

Moreover, the Government chose to use for-profit, closed-source proprietary software from a company that hired prosecutors from this case, rather than open-

[202] A. 6912; A. 6930.

[203] Fed. R. Crim. P. 16 Advisory Committee's Notes to 1966 Amendment.

source software.[204] The Government made an issue in the District Court about the alleged dangers exposing the source code, and how criminals could game the source code. However, there are many open-source programs, like Signal's encrypted messaging platform, that are both open source and not exploited by criminals.

To the extent that the Government took the position that "national security" required the non-disclosure of the information vital to confronting and challenging the Reactor analyses, it failed to put forth any evidence to that effect. The assumption that Sterlingov would use the information to develop countermeasures to Reactor's attributions, and that as the operator of Bitcoin Fog he had already attempted to do so, was an improper assumption of guilt, as well as an assumption of future criminal activity.[205]

Finally, the Government cannot meet its burden to demonstrate that preclusion of the requested source code and underlying heuristics and external intelligence data was harmless error. Without the clustering attribution outputs, the experts would have been unable to know where to start or end their blockchain tracing. They were critical to the ultimate conclusions, without which the experts

[204] A. 358 (Chainalysis lawyer stating that AUSA Youli Lee, an original prosecutor on this case, now is a lawyer for Chainalysis.).

[205] *See* A. 6892; A. 6935.

could not have supported their testimony. Had Sterlingov been afforded access to the inputs behind these clustering conclusions, he could have mounted a vigorous defense that cut to the heart of the Government's expert evidence.

C. Denial of Reactor Discovery Violated Appellant's Due Process Rights to Put on a Complete Defense

The right of a defendant to present a complete defense is one of "the most basic ingredients of due process of law."[206] It includes the defendant's ability to meaningfully test the evidence presented against him, and to affirmatively present favorable evidence.[207] In certain cases, the right may give way to "other legitimate interests in the criminal trial process."[208] But "evidence rules that infringe upon a weighty interest of the accused and are arbitrary or disproportionate to the purposes they are designed to serve" cannot supersede the rights of the Defendant.[209]

As the Supreme Court has held, "[t]he Due Process Clause of the Fifth Amendment provides defendants with 'a constitutionally protected privilege to

[206] *Wash. v. Texas*, 388 U.S. 14, 18 (1967).

[207] *Id*. at 19.

[208] *Chambers v. Mississippi*, 410 U.S. 284, 295 (1973).

[209] *Holmes v. South Carolina*, 547 U.S. 319, 324 (2006).

request and obtain from the prosecution evidence that is either material to the guilt of the defendant or relevant to the punishment to be imposed.'"[210]

"Constitutional materiality" means the evidence must "both possess an exculpatory value . . . and be of such a nature that the defendant would be unable to obtain comparable evidence by other reasonably available means."[211]

As argued above, the underlying inputs behind Reactor's clustering and attribution conclusions are exculpatory. The source code and heuristics would likely reveal systematic errors in blockchain attribution through over-inclusion (the algorithms erroneously group unrelated addresses), failure to account for privacy-preserving technologies like CoinJoin or PayJoin, that legitimately commingle transactions, or arbitrary threshold determinations that lack empirical validation. Indeed, the Government's expert conceded that Chainalysis and its competitors reach different clustering conclusions from identical blockchain data.[212] The heuristics themselves, not just their application, define critical points on the tracing map leading to or from an attribution.

[210] *U.S. v. Quinones*, 236 F. Supp. 3d 375, 377 (D.D.C. 2017).

[211] *Id*. at 377.

[212] A. 4142.

Moreover, unverified external intelligence data (Heuristic 3) retrieved through law enforcement seizures and unknown additional sources raise concerning issues of whether such data was outdated, erroneous, or based on flawed initial assumptions. Reactor's attributions, therefore, are only as good as these initial inputs. It's entirely possible that the external data from Heuristic 3 has created circular attribution chains where incorrect initial attributions propagate throughout Reactor's later attributions. Without the ability to verify the data in this Heuristic, Sterlingov could not adequately raise these issues of validity.

This precluded evidence was impossible to replicate through other means, due to its proprietary and black-box nature. Sterlingov could not reverse-engineer how Reactor reached specific clustering conclusions from the public blockchain alone. As previously stated, different tools produce different clustering attribution results. Other tools would lack Chainalysis's proprietary data sets.

Simply put, "the right to present a defense encompasses the right to fully evaluate the scientific evidence used against the defendant."[213] The Government's position that a defendant must accept machine generated evidence against him on faith violates due process. The District Court's denial of access because of

[213] *Commonwealth v. Skundrich*, No. 1246 WDA 2023, 2024 WL 4792912, at *9 (Pa. Super. Ct. Oct 22, 2024).

speculative future harm to a for-profit, third-party, forensics service provider improperly elevated commercial interests and investigative convenience over Sterlingov's due process rights to exculpatory evidence necessary to mount a complete defense.[214]

IV. The District Court Erred by Admitting Evidence of Child Pornography

The District Court abused its discretion in admitting testimony and documentary evidence that roughly $989 in post-mixed Bitcoin was sent by unknown Bitcoin Fog users to the South Korean child-pornography site Welcome to Video. This is approximately 0.00025% percent of the service's $400 million volume.[215] The Government presented no evidence that Sterlingov ever accessed, knew of, or benefited from that site, yet the court allowed this highly inflammatory evidence – allegedly tying him to pedophiles and child-pornographers – to reach the jury without any limiting instruction. During summation, the Government argued that Sterlingov helped these child pornographers;

> people like Billy Bob 1337 and Slammer 88 who used Bitcoin Fog to buy access to child sexual abuse material on sites like Welcome to Video. And when Welcome to Video was taken down and law enforcement was working to identify its users, those who used Bitcoin Fog were able

[214] *See, e.g.*, *State v. Arteaga*, 296 A.3d 542, 554-55 (N.J. Super. Ct. App. Div. 2023).

[215] *See*, A. 5363-69; A. 7222-52; A. 4082-98.

> to disappear back into the Fog, just like the defendant intended.[216]

Because the evidence added nothing to the disputed issues, it was at most marginally probative, adding little beyond emotional baggage. It should have been excluded under *Old Chief* and Fed. R. Evid. 403.[217]

The Welcome to Video evidence was needlessly cumulative of other evidence related to Bitcoin Fog's users.[218] Count One charged a conspiracy between Sterlingov, darknet vendors, and market administrators, but does not include Welcome to Video or its users as co-conspirators.[219] The Government introduced extensive evidence of darknet site users using Bitcoin Fog – the core of its case. By contrast, the value of Bitcoin that went to Welcome to Video after it had been mixed through Bitcoin Fog was statistically and substantively trivial. Nor was there any

[216] A. 6163.

[217] *Old Chief v. U.S.*, 519 U.S. 172 (1997).

[218] *See e.g.,* A. 7221 (direct transactions tied to Welcome to Video amounted to only $989, whereas other darknet marketplaces totaled $20,848,971).

[219] *See* A. 6561-64; A. 6832.

evidence that the operator of Bitcoin Fog knew or could have known what the Bitcoin was going to be used for after it had left the mixer.[220]

The only ostensible relevance of the Welcome to Video evidence was to a portion of Count Three, which included, in addition to regulatory based violations under 18 USC § 1960(b)(1)(A) and (b)(1)(B), a violation of (b)(1)(C).[221] Yet even for subsection (b)(1)(C), the Government did not need Bitcoin Fog users sending post-mix Bitcoin to a child pornography vendor to prove that users mixed criminal proceeds through Bitcoin Fog; the darknet market user mixes already evidenced that.[222] Nor does anything related to the Welcome to Video users go to attribution as to the identity of the operator of Bitcoin Fog, or to the operation of Bitcoin Fog. It is highly prejudicial. When Sterlingov's extensive devices were seized at his arrest, there was no child pornography anywhere. Accordingly, the evidence's minimal to

[220] The only other mention of child pornography was an unrelated internet forum post, made before Bitcoin Fog existed, condemning child pornography distribution through Tor. *See*, A. 3118; Gov. Ex. 55A. Although the Government attributed the post to Sterlingov, the post makes no mention of Welcome to Video and offers no evidence that Sterlingov knew of, intended to promote, or in any way supported such conduct.

[221] *See* A. 6561; 18 U.S.C. § 1960(b)(1)(A)–(C).

[222] *U.S. v. Cunningham*, 694 F.3d 372, 389 (3d Cir. 2012).

non-existent probative value should have placed it on the chopping block when weighed against its prejudice.

A. The Evidence Violates Fed. R. Evid. 403

Rule 403 directs courts to exclude evidence whose unfair prejudice "substantially outweighs" its probative value.[223] Few topics inflame juries more than child sexual abuse.[224] By tethering Sterlingov to child-porn purchasers, the Government invited the jury to punish him for repugnant conduct he neither committed nor intended. "[U]nfair prejudice" in the Rule 403 context means an "undue tendency to suggest decision on an improper basis, commonly, though not necessarily, an emotional one."[225] In a criminal trial, this refers to evidence that "lure[s] the factfinder into declaring guilt on a ground different from proof specific to the offense charged."[226] Here, the child sexual abuse content was exactly the sort of evidence that risks a verdict tainted by improper considerations. Introducing such incendiary matter effectively painted Sterlingov with the brush of a pedophile facilitator, even though the actual charges concerned money laundering and

[223] Fed. R. Evid. 403.

[224] *See, e.g., U.S. v. Loughry*, 660 F.3d 965, 972 (7th Cir. 2011).

[225] Fed. R. Evid. 403 Advisory Committee's Notes to 1975 Amendment.

[226] *Old Chief v. U.S.*, 519 U.S. 172, 180 (1997).

unlicensed money transmitting. The spillover prejudice was unavoidable and extreme.

In the Rule 403 balance, the fact that the post-mix amount sent to Welcome to Video was trivial cuts against admissibility: evidence of a tiny, isolated aspect of the alleged conduct tends to be less probative of the overall crimes, yet it can still inflame the jury just as much as (or more than) evidence of the core conduct. The District Court, however, inverted its Rule 403 analysis. Rather than recognizing that the little dollar value of the "Welcome to Video" usage undercut its probative worth, the court reasoned that the "minimal amount" was "favorable to the defense" and therefore concluded "I don't think it's a 403 problem."[227] This was an abuse of discretion. The court treated the small scale of the evidence as though it minimized the risk of prejudice, when in fact the small scale minimized its probative value. The prejudice – rooted in the shocking nature of child pornography – remained high, regardless of whether the jury was told it comprised only $989 out of $400 million. Informing the jury that the child porn was just a drop in the bucket did little to neutralize the visceral impact; if anything, the jury may have reasoned that even a small link to such depravity warranted punishment.[228]

[227] A. 4084.

[228] *Loughry*, 660 F.3d at 974.

The decision in *Old Chief* underscores the error here: courts must weigh not only the logical relevance of evidence but also whether other, less prejudicial means can establish the same point. If an alternative proof has "substantially the same or greater probative value" with lower unfair prejudice, the more prejudicial evidence should be excluded.[229] Here, the Government had abundant, alternative evidence of Bitcoin Fog users mixing illicit funds to make their case for the § 1960(b)(1)(C) offense.[230] The tiny increment of probative value contributed by Welcome to Video was far outweighed by its capacity to lure the factfinder into declaring guilt on an improper basis.

Moreover, the Government's presentation of the evidence and the court's handling of it magnified its prejudicial impact. First, the danger of unfair prejudice was amplified when the Government presented the bulk of the child-pornography evidence along with the corresponding exhibits through its last witness, Special Agent Steven Santell.[231] Second, because the defense had objected vigorously, the

[229] *Old Chief,* 519 U.S. at 183.

[230] *See U.S. v. Cunningham*, 694 F.3d 372, 389 (3d Cir. 2012).

[231] A. 5363-69. The Government likewise introduced the evidence earlier in the trial through Scholl. A. 4082-98. *See Loughry*, 660 F.3d at 974 ("increasing the risk of prejudice [], the Government introduced the 'hard core' pornography during the testimony of its final witness, shortly before the jury was excused to deliberate").

court was on notice of the need for careful limiting instruction. Yet the trial court gave no contemporaneous limiting instruction, and the final charge contained no specific guidance restricting the jury's use of this inflammatory evidence.[232] In the absence of such guidance, jurors were likely to let their revulsion spill into their consideration of every count.[233] This omission and the evidence's presentation compounds the Rule 403 error.

The improper admission of the Welcome to Video child-pornography proof was anything but harmless in this close case. Identity, whether Sterlingov actually operated Bitcoin Fog, was the trial's fulcrum, and the Government's attribution evidence was dated, wholly circumstantial, and fiercely disputed. Instead of resting

[232] To mitigate prejudice and spare the jury from viewing the footage, the Defense agreed – without independent confirmation that the files contained child pornography – to stipulate that the videos constituted a violation of 18 U.S.C. § 1466A:

MR. EKELAND: And if I understand the Court correctly, the Court is saying you would screen child pornography for the jury?

THE COURT: You know, it happens -- if we had to, if it got to that point, I don't know. If it really is disputed that these sites were actually child porn -- and I think Mr. Brown is right, you did yourself just a second ago say it hasn't been authenticated as child porn, so if that's disputed in the case, then I suppose that's the case. It's horrific, but it happens in cases. And, you know, I feel horrible for the jury to have to put them through that. But if it is a disputed fact, the Government is entitled to carry its burden on that.

A. 4414-15; *see also,* A. 5311-12.

[233] *See Loughry*, 660 F.3d at 975.

on that fragile footing, the prosecution injected emotionally charged proof designed to paint Sterlingov as a willing facilitator of child exploitation, parading twelve exhibits through two witnesses, including its very last witness, to leave the jury with a searing final image of depravity.[234] An evidentiary error is deemed harmless only if the verdict was "surely unattributable to the error."[235] In a close case hinging on circumstantial attribution, there is no such assurance here; the inflammatory and confusing Welcome to Video material almost certainly swayed the jury, creating precisely the type of unfair prejudice Rule 403 and the harmless-error doctrine condemn.

B. The Welcome to Video Evidence Constructively Amended the Indictment

Finally, the Government's reliance on the Welcome to Video evidence amounted to a constructive amendment of the indictment, infringing Sterlingov's Fifth Amendment right to be tried only on charges returned by the grand jury. Count One alleged a conspiracy with darknet *drug vendors* and *administrators*; it does not

[234] A. 7222-52.

[235] *U.S. v. Wilson,* 605 F.3d 985, 1024 (D.C. Cir. 2010); *see Kotteakos v. U.S.*, 328 U.S. 750, 765, (1946).

encompass *customers*, let alone patrons of a child-pornography site.[236] By introducing Welcome to Video evidence without a limiting instruction, failing to clarify its purpose at summation, and portraying those buyers as being aided by Bitcoin Fog, the Government impermissibly broadened the scope of Count One, which independently requires reversal.[237]

Because the District Court admitted highly inflammatory but minimally probative child-pornography evidence, failed to give a limiting instruction, and allowed the Government to impermissibly expand the charged conspiracy, it violated

[236] Because the funds in question moved only from Bitcoin Fog to the Welcome to Video site, they did not constitute criminal proceeds; instead, unbeknownst to Sterlingov, they were later (following their flow through Bitcoin Fog) used by others to purchase alleged child-pornography.

[237] *See Stirone v. U.S.*, 361 U.S. 212, 219 (1960); *U.S. v. Riley*, 115 F.4th 604, 615 (D.C. Cir. 2024). Abandoning the confines of its indictment, the Government expanded the alleged conspiracy to encompass individual buyers:

THE COURT: I am just continuing to think about the hearsay issue and as it relates to the records that have come in this morning. And my understanding is that the alleged conspiracy was between Sterlingov and anyone else who was involved in administering or running Bitcoin Fog and the vendors -- darknet vendors or vendors; correct?

MS. PELKER: Anyone who was using Bitcoin to launder narcotics trafficking proceeds and activities. So the darknet market administrators, the vendors. We would say the buyers are also in furtherance of that.

A. 5312-13.

Fed. R. Evid. 401 and 403 and Sterlingov's Fifth and Sixth Amendment rights. The conviction must be vacated.

V. The Trial Court Erred in Instructing the Jury on Willful Blindness

In its final instructions to the jury, the District Court included, over objection, a charge on the controversial and disfavored doctrine of willful blindness.[238] Also called "deliberate ignorance," "conscious avoidance" or an "ostrich instruction," willful blindness generally "equat[es] deliberate ignorance" of highly suspicious facts with actual "knowledge" of them.[239] Here, for example, the court told the jury:

> In considering whether the defendant had knowledge of a fact, you may consider whether he deliberately closed his eyes to what otherwise would have been obvious to him … [W]hen knowledge of the existence of a particular fact is an element of an offense, such knowledge can be established if a person has a subjective belief of a high probability of its existence, unless he actually believes that it does not exist.
>
> Thus, other knowledge on the part of the defendant cannot be established merely by demonstrating the defendant was negligent, reckless, careless or foolish. Knowledge can be inferred if the defendant deliberately blinded himself to the existence of a fact that he believed to a high probability of certainty existed.[240]

[238] *See, e.g.,* A. 6106-08.

[239] *U.S. v. Lee*, 966 F.3d 310, 323-24 (5th Cir. 2020).

[240] A. 6265*; see also,* A. 6275 ("This knowledge requirement" – that laundered funds were illegally derived – "includes instances of willful blindness.").

Although the Supreme Court has "approved the concept" of willful blindness, this Court and others warn that it should be charged "rarely," "sparingly" and with great "caution."[241] Relevant here, that's because the doctrine threatens to dilute the Government's burden of proof, raising due process and fair trial concerns under the Fifth and Sixth amendments. As Justice Kennedy put it: "Willful blindness is not knowledge; and judges should not broaden a legislative proscription by analogy."[242]

Mindful of these perils and admonitions, courts including this one have "emphasized" that a "deliberate ignorance instruction should be given *only* when a defendant claims a lack of guilty knowledge and the proof at trial supports an

[241] *Lee*, 966 F.3d at 324 (citing *U.S. v. Alston-Graves*, 435 F.3d 331, 340-41 (D.C. Cir. 2006); *see also Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754 (2011); *see, e.g., Cooper v. NTSB,* 600 F.3d 476, 483-84 & n.6 (D.C. Cir. 2011) (citing both *Alston-Graves* and *Global-Tech* as good law); *Tantchev v. Garland*, 46 F.4th 431, 437-38 & n.3 (6th Cir. 2022) (indicating that *Alston-Graves* survives *Global-Tech*, remains good law in this Circuit and "may require *more* than willful blindness to sustain a conviction for an offense that … requires 'knowledge'").

[242] *See U.S. v. Jewell,* 532 F.2d 697, 706 (9th Cir. 1976) (Kennedy, J., dissenting) ("When a statute specifically requires knowledge as an element of a crime, however, the substitution of some other state of mind cannot be justified even if the court deems that both are equally blameworthy."); *see also Global-Tech*, 563 U.S. at 772 (dissenting op.) (denouncing temptation to "distort" cases of willful blindness "into cases of knowledge"); *Alston-Graves*, 435 F.3d at 337 ("It makes obvious sense to say that a person cannot act 'knowingly' if she does not know what is going on. To add that such a person nevertheless acts knowingly if she intentionally does not know what is going on is something else again."); *id.* n.1 ("it is hard to see how ignorance, from whatever cause, can be knowledge").

inference of deliberate ignorance."[243] The latter requires a showing that the defendant took "deliberate actions" – meaning "active efforts," "deliberate steps" or "proactive steps" – to "avoid learning" the truth.[244] Because neither condition existed here, the charge was given in error.[245]

A. Charging Willful Blindness was Inappropriate Because Sterlingov Never Disclaimed Guilty Knowledge

First, although a willful blindness charge is improper unless the defendant denies culpable knowledge, Sterlingov never claimed ignorance that Bitcoin Fog served as a mixer for illicit criminal proceeds. [246] To the contrary, Sterlingov testified, and defense counsel argued, that he was not involved in Bitcoin Fog at all – that he played no role whatever in the platform's operation, management or control. The defense thus centered on identity and participation rather than state of mind, offering the jury a binary choice: either Sterlingov ran Bitcoin Fog or he didn't. If so, he knew what it was up to and he was guilty; if not, he was innocent.[247]

[243] *Lee*, 966 F.3d at 324 (emphasis added).

[244] *Global-Tech*, 563 U.S. at 769-771; *Lee*, 966 F.3d at 326 ("The key is whether there is evidence showing the defendant took proactive steps to ensure his ignorance.").

[245] The instruction's propriety is reviewed for abuse of discretion. *Lee*, 966 F.3d at 324.

[246] *Lee*, 966 F.3d at 324 (emphasis supplied).

[247] Cf. *Alston-Graves*, 435 F.3d at 341-42.

In these circumstances – where knowledge is undisputed or the evidence of it substantial – it's fundamental that conscious avoidance doesn't apply, and charging on the theory was erroneous.[248]

The Government's own summations illustrate the point. The prosecutors urged that Sterlingov "absolutely" and "certainly knew" that "huge amounts" of "dirty money" were "going through Bitcoin Fog."[249] In fact, the Government maintained, Sterlingov "specifically designed," "set up" and "built" the platform for that "very" purpose – to help "serious criminals" move and "hide their [ill-gotten] assets."[250] Indeed, the prosecutors even insisted that Sterlingov openly "stated" as much, asserting that he *admittedly* created Bitcoin Fog to "launder money" by "mix[ing] illegal fund activity from the darknet."[251] As the Government bluntly

[248] *See, e.g., Lee*, 966 F.3d at 324-25 (deliberate ignorance instruction potentially warranted "[w]ith knowledge in dispute"); *id.* at 326 (deliberate ignorance instruction "improper" when Government case "premised" on "actual knowledge"); *Alston-Graves*, 435 F.3d at 340-41.

[249] A. 6192; A. 6202; A. 6163.

[250] A. 6163; A. 6198; A. 6202.

[251] A. 6161; A. 6240.

contended: “Bitcoin Fog was a money laundering site, plain and simple. *Its stated and entire purpose for existing was to launder money*.”[252]

According to the prosecution, for example, Sterlingov was an “early user of Silk Road” who “understood the need for anonymity. … [He] knew what the darknet was for. … He had various messages and chats about his knowledge of exactly what the darknet was for. He used it himself.”[253] Armed with this knowledge, Sterlingov, on the Government’s theory, “wanted Bitcoin Fog to be a site for people who have real problems with the law. He knew that if a site could be traced back to him, people might go to jail.”[254] Thus “kn[o]w[ing] that he would be in trouble if this site were linked back to him” – “kn[ow]ing the authorities would be watching” – “[t]hat is why [Sterlingov] did this,” the Government alleged.[255] “That is why he came up with this plan. … Bitcoin Fog was about laundering money for darknet markets.”[256]

[252] A. 6193 (emphasis supplied); *see also* A. 6093 (prosecutor telling the District Court, “the defendant’s Killdozer account posted that the entire Bitcoin network is ‘plausibly deniable money laundering’”).

[253] A. 6153; A. 6241; *see also* A. 6093 (prosecutor telling the District Court, “it is *undisputed* that the defendant had a Silk Road account that he used to purchase psychedelic drugs”) (emphasis supplied).

[254] A. 6154.

[255] A. 6154; A. 6157.

[256] A. 6241; A. 6157.

To that end, the Government continued, Sterlingov purportedly wrote in online forums – in his "own" ostensible "words" – that the platform's users were:

> Criminals. … [P]eople with real problems with the law, people who would go to jail if the server were found, people who wanted to avoid the authorities. That is the user base the defendant wanted. That is what he designed Bitcoin Fog for. And that is what he got. …[257]
>
> He had set up Bitcoin Fog for people with real problems with the law, who would go to jail if their transaction information were revealed. *And he talks repeatedly about all the things he's doing to hide from the authorities*. …
>
> And, again, how do you know the defendant did this? Because that's what Bitcoin Fog was intended to do. *The defendant says so*. He is going to extreme lengths to help his customers hide from the authorities, to conceal their transactions, and to promote their activity. To contribute to their prosperity and his prosperity in the process.[258]

Driving home what it cast as his written admissions of knowledge – via its unscientific IP Overlap Analysis – the Government went on to ascribe to Sterlingov another online post that said: "'Stop struggling and get a Tor hidden service. For

[257] A. 6161-62.

[258] A. 6161-62; A. 5192-93.

years drugs are sold and unfortunately child pornography distributed through it."[259] Similarly, the prosecutors highlighted another post that read:

> There is no 100 percent protection from anything at all – this, by the way, is a month before he opens up Bitcoin Fog – there are only levels of probabilities that you will be found. As far as I understand, that's why you want a VPN.
>
> The more money you launder, the darker the schemes you crank out, the more information about you is leaking out to the network, et cetera, the higher is this probability. You can read all of it. The more you do to isolate yourself from what you're doing, the better off you'll be.
>
> It is, as the defendant said, up to you.[260]

Finally, leaving no room for doubt as to the import and primacy of these written attributions, the Government closed its rebuttal speech with a pregnant exhortation: "[T]ake a close look at who he's talking about when it comes to taking security precautions. Akemashite [a putative alias attributed to Sterlingov via the unscientific IP Overlap Analysis] only got to his referring to the users of Bitcoin Fog [sic]. He's not talking about himself."[261]

[259] A. 6162-63; *see also,* A. 6159 (alleging Sterlingov was "obsessively disciplined in hiding himself online. He used Tor, VPN and proxies for all of his internet communications.").

[260] A. 6242-43.

[261] A. 6246; *see also,* A. 6093 (prosecutor stating, "The Akemashite Omedetou posts are rife with references to using Bitcoin Fog to protect criminal activity.'").

Faced with this cache of actual knowledge evidence, meanwhile, the Defense countered that the evidence was consistent with Sterlingov having merely used – but not operated – Bitcoin Fog. And merely "[u]sing a mixer is legal," Defense counsel emphasized, absent any claim that Sterlingov had partaken in predicate criminality. Tellingly, the Defense did *not* suggest that Sterlingov was unaware the service could be or was used to "launder [dirty] money."[262]

On this record, with significant, uncontested evidence of actual knowledge and issue joining on the identity of Bitcoin Fog's purported principal, injecting the concept of willful blindness amounted to gratuitous and unnecessary overkill, the Government purely piling on. Put more colorfully, the Government misused "deliberate ignorance" as a "backup or supplement" when its case "genuinely hing[ed]" on Sterlingov's "actual knowledge" that Bitcoin Fog mixed tainted funds.[263] Willful blindness was wrongfully charged on this ground alone.

B. Charging Willful Blindness was Inappropriate Because Sterlingov Took No Deliberate Actions to Avoid Acquiring Guilty Knowledge

The District Court erred in charging willful blindness for another independent reason: there was no evidence that Sterlingov made "active efforts" aimed at, or took

[262] *See, e.g.*, A. 6222-26.

[263] *U.S. v. Lee*, 966 F.3d 310, 326 (5th Cir. 2020).

"proactive steps" for the purpose of, confirming any suspicions that Bitcoin Fog was laundering criminal proceeds. [264]

In attempting to marshal evidence satisfying this second and separate *Global-Tech* requirement, the Government pointed the court to (1) Bitcoin Fog's "purg[ing]" transaction logs "after one week"; and (2) the platform's "user interface" having been "designed not to collect any identifying information" as to its clientele or the "transactions" they conducted, including their "nature" and "location."[265]

The Government echoed these themes in summation, similarly arguing to the jury:

> Like any good money launderer, the defendant designed Bitcoin Fog to avoid learning unnecessary details of his customers' crimes. He set up his service to automatically delete logs. He added features to allow people to delete their messages and transaction history. He even deliberately designed his site to avoid collecting even basic records of its users. Even if they wanted to, users couldn't even add an email address to allow for password resets. That was all done intentionally by the defendant.[266]

[264] *Global-Tech*, 563 U.S. at 770; *Lee*, 966 F.3d at 326.

[265] A. 6093-97.

[266] A. 6202.

But the Government's own case theory flatly belies these specious assertions. The Government never claimed Sterlingov took these purported steps to "avoid learning" that Bitcoin Fog was washing dirty money.[267] Quite the opposite. According to the prosecutors themselves, Sterlingov "absolutely" and "certainly" knew Bitcoin Fog was doing just that, having "specifically designed" the platform for that precise if not "stated" purpose: to serve as "the highest possible anonymity outpost in the Bitcoin world, a place for serious criminals with real problems with the law to hide their money."[268]

Even better, the Government told the jury, Sterlingov had expressly advised the site's users in an online forum (again attributed to Sterlingov through the IP Overlap Analysis):

> "The more money you launder, the darker the schemes you crank out, the more information about you is leaking out to the network, et cetera, the higher is this probability [that you will be found]. … The more you do to isolate yourself from what you're doing, the better off you'll be."[269]

[267] *Global-Tech*, 563 U.S. at 769.

[268] A. 6150.

[269] A. 6242-43.

And that, said the prosecutors, was why Sterlingov implemented the service's "security precautions."[270] To "protect" the "us[e]" of Bitcoin Fog as a platform that he purposely designed and intended to facilitate "criminal activity."[271] *Not* to close his eyes to the fact that the site was being so used.

Because a "deliberate ignorance instruction" is "improper" when the Government "premise[s] its case on actual knowledge," resort to the theory here was thus a classic red herring. [272] Try as it might, the Government can't have it both ways.

The District Court decided to give the charge on a different rationale. While explicitly "*not* saying that it was done here," the court began by opining that willful blindness is or "could be" inherent in the "nature of a [crypto] mixer itself," because "the whole point of the mixer is to not know who the transactions are coming from or who they're going to."[273] The "alleged conduct" at issue, the court then went on to repeat for emphasis, "involved obfuscating who it was we were dealing with," adding that the service also "was marketed on that ground."[274] And in the court's

[270] A. 6246.

[271] A. 6093.

[272] *U.S. v. Lee*, 966 F.3d 310, 326 (5th Cir. 2020).

[273] A. 6066-67 (emphasis supplied).

[274] A. 6103.

ultimate view, "the entire nature of the alleged conspiracy and alleged criminal conduct here, which was founded on the notion of blindness and not knowing who you are dealing with," made the charge peculiarly "appropriate" in "this sort of case."[275] The court's approach misconstrues both the law of conscious avoidance and the nature and legal status of cryptocurrency mixing services. It also contradicts the Government's interpretation and the court's own holding that mixers are not *per se* illegal.[276]

First, the court appears to have performed a categorical analysis focused on what it considered the nature of the crime alleged and the sort of case presented. But the proper inquiry requires an individualized assessment of the defendant's own behavior, asking whether *he* took "deliberate actions" – meaning "active efforts," "deliberate steps" or "proactive steps" – to *personally* "avoid learning" or confirming suspicious facts.[277]

[275] A. 6109-10.

[276] *See, e.g.,* A. 6224; A. 6240; A.6705; Hrg. Tr. at 45:3 Oct. 25, 2021 ("There's nothing per se illegal about mixing Bitcoins" AUSA C. Brown); A. 3718.

[277] *Global-Tech*, 563 U.S. 769-71; *Lee*, 966 F.3d at 326 ("The key is whether there is evidence showing the defendant took proactive steps to ensure his ignorance.").

Yet the judge expressly did *not* so find as to Sterlingov, pointedly noting he was "*not* saying that it was done here."[278] The closest the judge came to such a finding was an observation that the site "*was* marketed" with an emphasis on its "obfuscating who it was we were dealing with."[279] But that speaks to Bitcoin Fog's public-facing outreach to potential customers, not to Sterlingov's own state of mind or any personal efforts to bury his head in the sand.

How a service is pitched to prospective consumers is not the kind of deliberate effort or proactive step to personally avoid guilty knowledge that willful blindness contemplates. In *Global-Tech*, the offending parties copied an overseas model of an innovative American product that bore no U.S. patent markings, also withholding from their own intellectual property lawyer that their version was "simply a knockoff."[280] No such deliberate attempts to "manufacture a claim of plausible deniability" of individual knowledge were alleged, proved or found by the District Court with respect to Sterlingov. [281] Anything imputed to him in this regard was "merely" a function of how the business operated in its ordinary course – a

[278] A. 6066-67 (emphasis supplied).

[279] A. 6103.

[280] *Global-Tech*, 563 U.S. at 770-71; *id.* 775 (Kennedy, J., dissenting).

[281] *Id.* 771 (maj. op.).

circumstance in *Lee* that "[fell] short" of the "compelling justification" and "purposeful contrivance required to raise an inference of deliberate ignorance" and rationalize a corresponding instruction.[282]

In supposing otherwise and issuing the charge anyway, the court effectively devised a blanket rule disfavoring cryptocurrency mixers and deeming them intrinsically suspect, authorizing automatic recourse to willful blindness in every case involving one. That *caveat emptor* construct is untenable. After all, both sides agreed that mixing activity is presumptively *legal* and legitimate, and the District Court so held.[283] What's more, at least one circuit has broadly recognized as much.[284]

Why? Crypto mixers, like such ubiquities as VPNs and WhatsApp, both preinstalled on every Apple iPhone, serve the salutary goal of promoting digital privacy. That is, all three protect users' personal identifying information and assets from hackers, other bad actors and threats, and – yes – even the prying eyes of the Government. And as any TV viewer knows, VPNs and WhatsApp are "marketed"

[282] *U.S. v. Lee*, 966 F.3d 310, 325-26 (5th Cir. 2020).

[283] *See, e.g.,* A. 6224; A. 6240; A.6705; A. 3718.

[284] *See generally, Van Loon v. Dep't of the Treasury*, 122 F.4th 549 (5th Cir. 2024).

to potential customers "on that [very] ground," just as the District Court said of Bitcoin Fog.[285]

Taken to its logical end, then, the District Court's reasoning would similarly sanction a willful blindness charge in any case involving the everyday use of a VPN or WhatsApp, online mainstays. It also defies the Justice Department's own recent guidance, in the Blanche Memo, directing Government lawyers not to prosecute – never mind seek ostrich instructions for – crypto mixers unless they "(a) cause financial harm to digital asset investors and consumers; and/or (b) use digital assets in furtherance of other criminal conduct, such as fentanyl trafficking, terrorism, cartels, organized crime, and human trafficking and smuggling."[286]

Contrary to the District Court's apparent impression, in sum, secrecy and anonymity are features – not bugs – of crypto mixers and other common online privacy tools such as VPNs and WhatsApp.[287] The court's rationale inverted this truism, so its willful blindness instruction was erroneous and cannot stand.

[285] A. 6103.

[286] A. 7218.

[287] *Cf.* A. 7217 (calling "digital assets industry … critical to the Nation's economic development and innovation," and stressing that "the Department of Justice is not a digital assets regulator").

C. The Errant Ostrich Instruction Worked Concrete Prejudice and Requires Reversal

In contrast to cases like *Alston-Graves* and *Lee*, the baseless ostrich instruction given here cannot be waved off as harmless error. First, the Government argued the issue at length in summation, forecasting the court's charge on the point but mangling the ostrich doctrine's thrust to squeeze the evidence into its four corners. In that vein, the prosecutor asserted:

> Judge Moss will instruct you that it's not a defense to deliberately cover your eyes and ears to avoid learning the truth. Think of an ostrich sticking its head in the sand. *Under the law*, if the defendant knew there was a high probability of Bitcoin Fog being used to move drug proceeds and he deliberately blinded himself to the *details* of those drug deals, that can be considered evidence of knowledge. He can't just stick his head in the sand.
> Like any good money launderer, the defendant designed Bitcoin Fog to avoid learning unnecessary *details* of his customers' crimes. …[288]

But conscious avoidance has nothing to do with *details*. And the money laundering *law*, 18 USC § 1956, doesn't concern itself with *details*, either. Rather, conscious avoidance speaks to defendants "deliberately shielding themselves from clear evidence of *critical facts* that are strongly suggested by the circumstances."[289]

[288] A. 6201-02 (emphasis supplied).

[289] *Global-Tech*, 563 U.S. at 766 (emphasis supplied).

For these purposes, the "critical facts" under the money laundering statute were whether Bitcoin Fog mixed illicit funds and Sterlingov knew it. If so, he was guilty; if not, he was innocent. Invoking willful blindness and conflating it with the details of the underlying drug deals only muddied the waters and inserted extraneous considerations, confusing the jury by garbling what the Government needed to prove.[290]

Second, the issue appears to have troubled the jury. That's because their lone note concerned the "knowledge requirement" of Count Four, alleging that Sterlingov ran an unlicensed D.C. money transmission business in violation of local law, asking if it applied to both operating the business and doing so within the District.[291] And the willful blindness charge, by its terms, covered all four counts of the indictment.[292]

Third, despite strenuously advocating for the charge, the Government shirked its concomitant responsibility to seek a special verdict on the knowledge issue.[293] That dereliction makes it impossible to determine which theory or theories of knowledge the jury relied on: actual knowledge, willful blindness or both. As a

[290] *U.S. v. Lee*, 966 F.3d 310, 326 (5th Cir. 2020).

[291] A. 6326.

[292] A. 6265.

[293] *See, e.g., U.S. v. Sturdivant*, 244 F.3d 71, 76 n.4 (2d Cir. 2001).

result, the Government cannot meet its burden to prove the instructional error harmless.[294]

The ostrich instruction in this case was unfounded because it lacked an appropriate factual predicate: evidence that Sterlingov both disclaimed guilty knowledge and took deliberate actions to avoid acquiring it. In addition, the errant instruction was demonstrably prejudicial. For these reasons, it derails Sterlingov's conviction and demands reversal.

VI. The Evidence Was Insufficient to Support the Conviction

At both the close of the Government's and Defense's cases, Defense counsel made oral motions for judgment of acquittal based on the insufficiency of the evidence. The court denied both motions.[295] A conviction must rest on evidence that permits a rational trier of fact to find each essential element of the crime beyond a reasonable doubt.[296] Even when the speculative, circumstantial evidence in this case

[294] *See, e.g., U.S. v. Simpson*, 430 F.3d 1177, 1183-84 (2d Cir. 2005).

[295] A. 5386; A. 6140.

[296] *See, e.g., Jackson v. Virginia*, 443 U.S. 307, 319 (1979).

is viewed in a light most favorable to the Government, it is insufficient for a rational trier of fact to find guilt beyond a reasonable doubt.[297]

VII. The Testimony of Lichtenstein and Harmon was Irrelevant and Highly Prejudicial

Over Defense objection, the District Court allowed the testimony of cooperating Government criminal witnesses Harmon and Lichtenstein, both admitted users of Bitcoin Fog who unequivocally denied knowing or interacting with Sterlingov.[298] Harmon had pled guilty to a money laundering conspiracy, operating an unlicensed money transmission business in violation of federal law, as well as the same D.C. municipal statute at issue in Sterlingov's case.[299] Indeed, the charges against Harmon were essentially the same ones levelled against Sterlingov, but that's where the similarities end. Harmon testified to running millions of dollars' through his own Bitcoin mixer, and only using Bitcoin Fog 8-10 times, but finding it clunky.[300] He also testified, in contrast to Sterlingov, that when he was arrested, the

[297] *See U.S. v. Long,* 905 F.2d 1572, 1576 (D.C. Cir. 1990) ("We must ensure that the evidence adduced at trial is sufficient to support a verdict as a matter of law. A jury is entitled to draw a vast range of reasonable inferences from evidence, but may not base a verdict on mere speculation.") (Thomas, J.).

[298] A. 4395-96.

[299] A. 5090.

[300] A. 5081-82.

Government found his private keys, as well as extensive evidence implicating him.[301] The prejudice and irrelevance was even worse when it came to Lichtenstein, a Russian similar in appearance to Sterlingov, who pled guilty to money laundering conspiracy for his multi-million hack and heist of the crypto exchange Bitfinex.[302] Lichtenstein testified he used Bitcoin Fog 5-10 times to mix between 1-5 Bitcoins.[303] Additionally, over objection, Lichtenstein and Harmon gave unnoticed and improper expert testimony in violation of Fed. R. Evid. 702 regarding, among other things, the operation of mixers.[304] Neither Lichtenstein nor Harmon testified to the operation of Bitcoin Fog, nor anything having to do with Sterlingov. [305] The Government's sole purpose in putting on these admitted felons was simply to taint Sterlingov with their criminality.

VIII. The District Court Erred in Admitting Co-Conspirator Evidence Without the Requisite Foundation Under Rule 801(d)(2)(E)

The District Court committed reversible error in admitting hearsay evidence of darknet markets and operator statements as purported co-conspirator statements

[301] A. 5091-92.

[302] A. 4363; A. 4422.

[303] A. 4437-38.

[304] *See, e.g.,* A. 4435.

[305] A. 5039-56.

without first requiring the Government to establish, by a preponderance of the evidence, the existence of a conspiracy, Sterlingov's knowing participation in it, and that the statements were made during and in furtherance of that conspiracy, as required by Fed. R. Evid. 801(d)(2)(E).[306] The Government failed to meet this foundational burden, relying instead on speculative clustering methodology and tenuous inferences rather than direct or circumstantial evidence of any agreement or relationship between Sterlingov and the alleged co-conspirators as listed in the Government's Bill of Particulars.[307]

A. The Government Failed to Prove a Conspiracy Involving Sterlingov

Rule 801(d)(2)(E) renders statements by a co-conspirator non-hearsay only if the Government establishes "(1) that a conspiracy existed; (2) that the declarant and the defendant were members of the conspiracy; and (3) that the statement was made during the course and in furtherance of the conspiracy."[308] These elements must be proven by a preponderance of the evidence.[309] While the statement may be considered when making this determination, it cannot by itself establish the

[306] *See, e.g.,* A. 3927-29.

[307] A. 6832.

[308] *See U.S. v. Gatling*, 96 F.3d 1511, 1520 (D.C. Cir. 1996); *U.S. v. Jackson*, 627 F.2d 1198, 1217 (D.C. Cir. 1980).

[309] *See Bourjaily v. United States*, 483 U.S. 171, 175–76 (1987).

existence of a conspiracy or a defendant's participation. Accordingly, the proponent must offer evidence independent of the statement showing a conspiracy existed in which the defendant participated.

Here, the Government failed at the threshold: it presented no evidence, direct or inferential, of an agreement between Sterlingov and any identified individual to engage in money laundering or other unlawful activity. The Government's theory relied almost entirely on conclusions drawn from Chainalysis Reactor, and offered no concrete evidence of communication, coordination, or shared criminal intent between Sterlingov and any other actor. Indeed, the Governemnt proffered no testimony from a single eye-witness. All of its testimony came from experts, investigators, irrelevant cooperating witnesses, or translators, years after the fact.

Even assuming that some users of darknet markets laundered money through Bitcoin Fog, there was no proof that Sterlingov knew these individuals, agreed to join their criminal activity, or knowingly furthered their objectives. As the D.C. Circuit has repeatedly held, "[t]he essence of a conspiracy is an agreement to commit [a specific] unlawful act."[310] Mere association or parallel conduct does not suffice.[311]

[310] *U.S. v. Treadwell*, 760 F.2d 327, 333 (D.C. Cir. 1985).

[311] *See U.S. v. Spinner*, 152 F.3d 950, 956 (D.C. Cir. 1998) (no conspiracy where "the evidence failed to show that [defendant] was aware of the overall scheme").

And as the Blanche Memo declares, DOJ will no longer prosecute mixer-operators for the crimes of their end-users.[312]

Allowing the Government to bootstrap the existence of a conspiracy from conduct that is equally consistent with innocent activity, such as operating an privacy service with legitimate uses, would render the protections of Rule 801(d)(2)(E) meaningless.

B. The District Court Abdicated Its Gatekeeping Role Under Rule 104(a)

The court failed to make a preliminary determination under Fed. R. Evid. 104(a) that the foundational elements of Fed. R. Evid. 801(d)(2)(E) were met. Instead, the court deferred entirely to the government's "tenable" theory of conspiracy and treated the evidence as "intrinsic" to the offense.[313] But as the D.C. Circuit has emphasized, a district court should make an explicit determination that the defendant joined the conspiracy before admitting statements under Rule 801(d)(2)(E).[314]

[312] A. 7217.

[313] *See* A. 2652-53.

[314] *U.S. v. Jackson*, 627 F.2d 1198, 1209 (D.C. Cir. 1980).

IX. Miscalculation of the "Value of the Laundered Funds" Under U.S.S.G. § 2S1.1(a)(2)

The Court applied 28 levels for the loss amount based on the $395,563,025.39 the Government claimed flowed through Bitcoin Fog (both the funds that the Government claimed flowed into Bitcoin Fog and the very same funds it claimed flowed out of Bitcoin Fog).[315] To determine the loss amount, however, a court must look to the amount of "laundered funds."[316] As relevant, the definition of "laundered funds" "corresponds with" an actual violation of 18 U.S.C. § 1956.[317] Money laundering under the relevant provisions of Section 1956 focuses on the initial "transaction by which one receives illicit funds."[318] Therefore, here, the "laundered funds" are the purported criminally derived funds originally injected or infused into the respective money laundering scheme.[319]

The court's loss calculation was erroneous. The Government failed to establish that Sterlingov and/or Bitcoin Fog knowingly received or transacted with

[315] *See, e.g.*, A. 7129-30.

[316] U.S.S.G. § 2S1.1(a)(2) (directing courts to determine the "value of laundered funds" that "corresponds to" an offense level in the table in U.S.S.G. § 2B1.1).

[317] *See U.S. v. Jordan*, 447 F. App'x 574, 576 (5th Cir. 2011); *U.S. v. Van Alstyne*, 584 F.3d 803, 817 (9th Cir. 2009); A. 7172.

[318] *U.S. v. Stanford*, 823 F.3d 814, 850 (5th Cir. 2016).

[319] *See, e.g.*, A. 7171-72; *id.* at 18 (citations omitted); *see also, e.g.*, A. 7176-78.

any criminal proceeds or funds represented to be criminally derived with the requisite criminal intent. No evidence was presented that Sterlingov or Bitcoin Fog knew what wallet addresses corresponded to darknet sites or knowingly received darknet funds. To the contrary, the Government's experts indicated their clustering process to be complex, where most of the darknet clusters were a result of applying proprietary information, as opposed to readily available public information.[320] Additionally, there are no memo lines on transactions/transaction requests, and Bitcoin Fog was not said to have access to or collect any personal user data beyond a username, wallet address, and login.[321]

The Court's calculation also conflicts with Section 2S1.1(a)(2)'s application notes.[322] The Commission's text is clear: even if legitimately derived funds are commingled with criminally derived funds, "the value of the laundered funds, for purposes of subsection (a)(2), is the amount of the criminally derived funds, not the total amount of the commingled funds," unless "the amount of the criminally derived

[320] *See generally, e.g.*, A. 6465-92.

[321] *See, e.g.*, A. 6474.

[322] Indeed, the government offered no actual evidence that the funds were commingled and claimed to have been able to trace illicit proceeds into and/or out of Bitcoin Fog. *See* Application Note 3 to U.S.S.G. § 2S1.1(a)(2).

funds is difficult or impracticable to determine."[323] Here, the Government quantified the criminally derived amount: even if we accepted the Government's analytics and its claim that all funds said to be from darknet markets should be deemed criminally derived funds, out of the $395,563,025.39 in purported Bitcoin Fog transaction volume, the Government only attributed $78,541,872 to known darknet markets.[324] Thus, the "difficult or impracticable" exception does not apply.

Assuming *arguendo* that the worst-case version of the facts are true, a court would only be able to conclude that, at most, the funds that were said to go into Bitcoin Fog provides the relevant amount (the Count Two Government payments sent into Bitcoin Fog and the $78,541,872 said to be sent into Bitcoin Fog of purported illict proceeds).[325] Though, as discussed throughout, the Government failed to prove the amounts it claimed were illicit proceeds or even the mere fact of whether funds were actually flowing through Bitcoin Fog.

[323] Application Note 3(B) to U.S.S.G. § 2S1.1(a)(2).

[324] *See* A. 7115.

[325] Though, the number would likely be much smaller, as the Government's own expert chart indicated that no more than $47 million constituted directly dirty money. *See* A. 7115. Under the District Court's calculation, the loss enhancement and one or more other enhancments cover the magnitude of the offense in a manner that is not intended and that constutites double, triple, etc., counting, respectively. *See, e.g.*, A. 7176-78.

Although advisory, the Guidelines remain the starting point and the selected range is the "anchor" and "lodestar" for the whole analysis, especially where the district court, prior to sentencing, sought information from the "U.S. Sentencing Commission . . . as to what sentences judges have imposed over the past fifteen years for convictions under 18 U.S.C. § 1956, where the relevant guideline is 2S1.1(a)(2) with a final offense level of 43."[326] Without any other changes to the Guidelines calculation and before any variances and departures, the proper computation under 2S1.1(a)(2) would have resulted in a total offense level between 40 and 42, providing a different "anchor" and producing a different disparity assessment, with a likely lower sentence consistent with similarly situated defendants.[327] Courts have recognized "the powerful anchoring effect of a miscalculated Guidelines range on a district court's thinking about the appropriate sentence."[328]Accordingly, an incorrectly calculated Guideline range is a "significant procedure error" that mandates vacatur and resentencing.[329]

[326] *See Molina-Martinez v. United States*, 578 U.S. 189, 199 (2016); Dist. Ct. Dkt. No. 326 at 1.

[327] A. 7178-86; Dist. Ct. Dkt. No. 335 at 1-2.

[328] *U.S. v. Seabrook*, 968 F.3d 224, 234 (2d Cir. 2020).

[329] *Gall v. U.S.*, 552 U.S. 38, 51 (2007); *see also Molina-Martinez*, 578 U.S. at 198; *U.S. v. Brown*, 892 F.3d 385, 400 (D.C. Cir. 2018).

X. The Statute of Limitations Has Run

The Government's prosecution of Sterlingov is barred by the applicable statutes of limitations, which are five years for Counts 1–3 and six years for Count 4. [330] The Superseding Indictment generally alleges that counts 1-4 started on or about October 27, 2011, and continued at least until April 27, 2021, in the District of Columbia and elsewhere.[331]

A. Standard of Review

A court reviews legal determinations related to statutes of limitations *de novo*, and factual determinations for clear error.[332]

B. There is Insufficient Evidence for Criminal Conduct Within the Applicable Statutes of Limitations

There is insufficient evidence to establish criminal conduct within the relevant statute of limitations. Almost all the darknet markets in question were shut down by the Government or ceased operations outside the statute of limitations.

[330] *See* 18 U.S.C. § 3282(a); D.C. Code § 26-1023(c) (2023); *id.* § 23-113(4) (2023).

[331] A. 6561.

[332] *See, e.g., U.S. ex rel. Miller v. Bill Harbert Int'l Const., Inc.,* 608 F.3d 871, 878 (D.C. Cir. 2010).

The Government introduced nine darknet marketplaces that sent funds directly to Bitcoin Fog, and one that did not (Welcome to Video). Silk Road was shut down by law enforcement in October 2013.[333] Sheep was shut down in 2013.[334] Silk Road 2.0 was shut down by law enforcement in November 2014.[335] Pandora Openmarket was taken down by law enforcement in 2014.[336] Agora was taken down by the site's administrators in 2015.[337] Abraxas was shut down in 2015.[338] Black Bank was shut down in 2015.[339] Nucleus went offline in 2016.[340] Alphabay was shut down by law enforcement in July 2017.[341] And Welcome to Video was taken down by law enforcement in 2018.[342]

Welcome to Video is irrelevant because it never interacted with Bitcoin Fog. As for Alphabay, the Government's expert Scholl testified that he was aware of no

[333] A.6411.

[334] A. 6415.

[335] A. 6411-12.

[336] A. 6414.

[337] A. 6413.

[338] A. 6414.

[339] A. 6415.

[340] A. 6413.

[341] A. 6412.

[342] A. 6416.

evidence of Sterlingov ever used Alphabay, and that there was no evidence that Sterlingov ever communicated with Alphabay administrators.[343] The same is true for all darknet markets, except for Silk Road where Sterlingov had a personal user account with only a few personal transactions well outside the statute of limitations when he was in Sweden.[344] Moreover, there is no evidence that Sterlingov would have known the purpose of any of the darknet transactions, even if he had the ability to identify them. Nor is there any evidence of any criminal activity involving Sterlingov and any darknet market within the requisite statute of limitations.

Despite this, over objection, the Government devoted substantial trial time to defunct markets, especially Silk Road, improperly prejudicing the jury with time-barred and irrelevant allegations.[345] The use of such evidence underscores the lack of admissible proof within the statutory period and highlights the Government's attempt to circumvent the statute of limitations (as well as unduly prejudice Sterlingov) through impermissible evidentiary overreach. Sterlingov's conviction should be vacated because there is no evidence of any crimes within the relevant statute of limitations.

[343] A. 4316.

[344] *See, e.g.*, A. 5237-38.

[345] *See, e.g.,* A. 5227 *et. seq.*

C. The Evidence was Insufficient to Establish any Continuing Offense

There were no communications or acts in furtherance of any criminal activity within the statutes of limitations. The Government's case relied on an unreliable forensics to tar Sterlingov with the Akemashite Omedatou pseudonym, an assumption that Sterlingov administrated Bitcoin Fog, an assumption that no other individuals were involved in the operation of the complex mixing service, and an assumption that Bitcoin Fog never changed hands.[346] These assumptions were incorporated into the Government's argument that there was a continuing course of conduct from 2011 through to the day of Sterlingov's arrest.

The Government produced no direct evidence at trial of any conspiratorial act or communication during the relevant time period, nor any evidence related to his purported actual operation of Bitcoin Fog during the relevant statute of limitations. There are no time stamped logs anywhere for Bitcoin Fog.

Moreover, the Government offered no evidence that Sterlingov received or read the messages accompanying the undercover transactions upon which the Government relies to justify the continuation of conspiratorial offences. Furthermore, the funds used by the IRS were not derived from a criminal enterprise.

[346] *See, e.g.,* A. 6222-23; A. 3078.

Because there is no evidence of any criminal conduct or act in furtherance thereof, in this District, by Sterlingov or any co-conspirator within the relevant statute of limitations, this Court should reverse and vacate the conviction.

ORAL ARGUMENT REQUESTED

Sterlingov respectfully requests oral argument because it will assist the Court in addressing the complex factual and legal issues presented.

CONCLUSION

For the foregoing reasons, this Court should reverse Sterlingov's conviction and vacate the judgment below.

Dated: September 15, 2025

Respectfully submitted:

/s/ Tor Ekeland
Tor Ekeland Law, PLLC
30 Wall Street
8th Floor
New York, NY 10005
(718) 737-7264
tor@torekeland.com

Attorneys for Appellant-Defendant
Roman Sterlingov

CERTIFICATE OF COMPLIANCE

Certificate of Compliance with Type-Volume Limit, Typeface Requirements and Type-Style Requirements.

1. This document complies with the type-volume limit of Fed. R. App. P. 32(a)(7)(B) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f): this document contains 19,940 words under the limit per Court's Order, dated August 14, 2025.

2. This document complies with the typeface requirements of Fed. S. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this document has been prepared in a proportionally spaced typeface using Microsoft Word (2019/Office) in 14-point font, Times New Roman.

/s/ Tor Ekeland
Tor Ekeland Law, PLLC
30 Wall Street, 8th Floor
New York, NY 10005
(718) 737-7264
tor@torekeland.com

Attorneys for Appellant-Defendant
Roman Sterlingov

CERTIFICATE OF SERVICE

I certify that I electronically filed the above with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit using the appellate CM/ECF system on September 15, 2025.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF System.

Dated: September 15, 2025

Respectfully submitted:

/s/ Tor Ekeland
Tor Ekeland Law, PLLC
30 Wall Street
8th Floor
New York, NY 10005
(718) 737-7264
tor@torekeland.com

Attorney for Appellant-Defendant
Roman Sterlingov